HINDI

Certified Ethical Hacker (CEH) Certification And Exam Guide v10

CERTIFIED ETHICAL HACKER (CEH) CERTIFICATION AND EXAM GUIDE V10 IN HINDI

www.cprogrammingbookinhindi.com

Certified Ethical Hacker (CEH) Certification and Exam Guide V10 in Hindi

Copyright © 2017 by Machhindra Kalan

All rights reserved. No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage or retrieval system, without the prior written permission of the copyright owner and the publisher.

Trademarked names may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, we use the names only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

Lead Editor: Machhindra Kalan

Distributed to the book trade worldwide by Web Study Lab Pvt Ltd, Location - Mumbai, Palava city Pin 421204

E-mail: machhi29@gmail.com, or

Visit: www.cprogrammingbookinhindi.com

For information on translations, please contact Web Study Lab Pvt Ltd, Location - Mumbai, Palava city Pin 421204

Phone +91 86555-67778

The information in this book is distributed on an “as is” basis, without warranty. Although every precaution has been taken in the preparation of this work, the author shall not have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this book.

This book
is dedicated
to those

who really wants
to be a

CERTIFIED ETHICAL HACKER (CEH) CERTIFICATION AND EXAM GUIDE V10 IN HINDI

INDEX OF CONTENTS

Table of Contents

INTRODUCTION

Chapter 1 Getting Started……..26
- Security
  - Essentials
  - Security Basics
- Introduction to Ethical Hacking
  - Hacking Terminology
  - The Ethical Hacker
- Questions
- Answers (sent your email)

Chapter 2 Reconnaissance……81
- Footprinting
  - Passive Footprinting
  - Active Footprinting
- Footprinting Methods and Tools
  - Search Engines
  - Website and E-mail Footprinting
  - DNS Footprinting
  - Network Footprinting
  - Other Tools
- Questions
- Answers (sent your email)

Chapter 3 Scanning and Enumeration……133
- Fundamentals
  - TCP/IP Networking
  - Subnetting
- Scanning Methodology
  - Identifying Targets
  - Port Scanning
  - Evasion
  - Vulnerability Scanning
- Enumeration
  - Windows System Basics
  - Enumeration Techniques
- Questions
- Answers (sent your email)

Chapter 4 Sniffing and Evasion……..216
Essentials
Network Knowledge for Sniffing
Active and Passive Sniffing
Sniffing Tools and Techniques
Techniques
Tools
Evasion
Devices Aligned Against You
Evasion Techniques
Questions
Answers (sent your email)

Chapter 5 Attacking a System…….282
Getting Started
Windows Security Architecture
Linux Security Architecture
Methodology
Hacking Steps
Authentication and Passwords
Privilege Escalation and Executing Applications
Hiding Files and Covering Tracks
Questions
Answers (sent your email)

Chapter 6 Web-Based Hacking: Servers and Applications…….349
Web Servers
Web Organizations
Attack Methodology
Web Server Architecture
Web Server Attacks
Attacking Web Applications
Application Attacks
Countermeasures
Questions
Answers (sent your email)

Chapter 7 Wireless Network Hacking…….409
Wireless Networking
Wireless Terminology, Architecture, and Standards
Wireless Hacking
The Mobile World
Mobile Platforms and Attacks

Mobile Attacks
Questions
Answers (sent your email)

Chapter 8 Security in Cloud Computing…….458
Cloud Computing
Cloud Security
Threats and Attacks
Questions
Answers (sent your email)

Chapter 9 Trojans and Other Attacks…….480
The “Malware” Attacks
Trojans
Viruses and Worms
Remaining Attacks
Denial of Service
Session Hijacking
Questions
Answers (sent your email)

Chapter 10 Cryptography……..527
Cryptography and Encryption Overview
Encryption Algorithms and Techniques
PKI, the Digital Certificate, and Digital Signatures
The PKI System
Digital Certificates
Digital Signatures
Encrypted Communication and Cryptography Attacks
Encrypted Communication
Cryptography Attacks
Questions
Answers (sent your email)

Chapter 11 Social Engineering and Physical Security…….587
Social Engineering
Human-Based Attacks
Computer-Based Attacks
Mobile-Based Attacks
Physical Security
Physical Security 101
Questions
Answers (sent your email)

Chapter 12 The Pen Test…….630
Methodology and Steps
The Security Assessments
Security Assessment
Deliverables Guidelines
More Terminology
Questions
Answers (sent your email)

INTRODUCTION

स्वागत है, प्रिय पाठक! मुझे पूरी उम्मीद है कि आपने इस परिचय के लिए अपना रास्ता खुशहाल, स्वस्थ और आत्मविश्वास से भरपूर किया है या, बहुत कम से कम, जिज्ञासा के साथ। मैं आपको वहां देख सकता हूं, किताब के माध्यम से आपके बुकस्टोर में खड़े होकर या किसी ऑनलाइन रिटेलर के वर्चुअल पेज पर क्लिक करके अपने लिविंग रूम में बैठे। और आप सोच रहे हैं कि क्या आप इसे खरीदेंगे– क्या यह वह पुस्तक है जिसे आपको अपने अध्ययन गाइड की आवश्यकता है। आपने संभवतः रूपरेखा का दुरुपयोग किया है, अध्याय के शीर्षकों की जाँच की है – आपने शायद यह भी पढ़ा होगा कि महान लेखक जैव ने मुझे लिखने के लिए मजबूर किया। और अब आप इस के लिए अपना रास्ता मिल गया है, निश्चित रूप से, इस परिचय को पुस्तक के और बहिष्कार को समझाने के लिए डिज़ाइन किया गया है – अपनी सुंदरता और चालाक बुद्धिवाद को इस तरह से बिछाने के लिए कि आप इसे खरीदने का विरोध नहीं कर सकते। लेकिन मैं भी एक पल लेने जा रहा हूं और स्थिति की वास्तविकताओं को समझाऊंगा और आपको बताऊंगा कि आप वास्तव में क्या कर रहे हैं।

यह पार्क में टहलना नहीं है। प्रमाणित एथिकल हैकर (सीईएच) ने प्रतिष्ठा हासिल नहीं की और इसे प्राप्त करना आसान होने से मूल्य है। यह एक चुनौतीपूर्ण Exam है जो केवल सरल याद रखने से अधिक परीक्षण करती है। इसके मूल्य ने इसे उच्च प्रमाणपत्रों में से एक के रूप में ऊंचा कर दिया है जो एक तकनीशियन प्राप्त कर सकता है, और यह DoD 8570 के DoD नेटवर्क पर प्रमाणीकरण के लिए कॉल का हिस्सा बना हुआ है। संक्षेप में, इस प्रमाणीकरण का अर्थ वास्तव में नियोक्ताओं के लिए कुछ है क्योंकि वे जानते हैं कि इसे प्राप्त करने के लिए किए गए प्रयास। यदि आप प्रयास में नहीं लगाना चाहते हैं, तो शायद आपको अध्ययन की एक और पंक्ति चुननी चाहिए।

यदि आप करियर क्षेत्र में नए हैं या आप उत्सुक हैं और अपने ज्ञान का विस्तार करना चाहते हैं, तो आप वहाँ खड़े हो सकते हैं, अपने चेहरे पर मासूम उम्मीद की चमक के साथ, इस इंट्रो को पढ़कर सोच रहे हैं कि क्या यह आपके लिए पुस्तक है। आपको तय करने में मदद करने के लिए, अपने प्रवेश चिह्न पर एक virtual सैर करें और एक नज़र डालें। चलो, आपने पहले एक देखा है– यह रोलर कोस्टर रीडिंग के सामने एक जैसा है, "आपको सवारी में प्रवेश करने के लिए यह लंबा होना चाहिए।" हालांकि, यह एक छोटा सा अलग है। आपकी ऊंचाई के बजाय, मुझे आपकी जानकारी में दिलचस्पी है, और मेरे पास आपके लिए एक या दो प्रश्न हैं। क्या आप OSI संदर्भ मॉडल को जानते हैं? डिफ़ॉल्ट रूप से एसएमटीपी किस पोर्ट का उपयोग करता है? टेलनेट के बारे में कैसे? Transport प्रोटोकॉल (टीसीपी या यूडीपी) वे क्या उपयोग करते हैं और क्यों? क्या आप संभवतः उन (Ports) पर कुछ और चला सकते हैं? RFC क्या है?

मैं ये सवाल क्यों पूछ रहा हूँ? खैर, मेरे नए virtual दोस्त, मैं आपको कुछ पीड़ा से बचाने की कोशिश कर रहा हूं। जैसे आपको एक रोलर कोस्टर पर अनुमति नहीं दी जाएगी, जो संभावित रूप से आपको कुछ पीड़ा और / या मौत में बहा सकता है, मैं खड़ा नहीं होने जा रहा हूं और आपको कुछ ऐसा करने के लिए तैयार नहीं हूं। यदि मेरे द्वारा पूछा गया कोई भी प्रश्न आपको अन्य रूप से प्रतीत होता है, तो आपको इस प्रमाणीकरण का प्रयास करने से पहले कुछ समय यांत्रिकी और नेटवर्किंग के आंतरिक कामकाज का अध्ययन करने में बिताना होगा।

मुझे गलत मत समझो–आगे बढ़ो और इस पुस्तक को खरीदो। आप इसे बाद में चाहेंगे, और मैं बिक्री संख्या का उपयोग कर सकता हूं। मैं यह कह रहा हूं कि इस प्लेट में कदम रखने से पहले आपको मूल

बातें सीखने की जरूरत है। मैंने इस पुस्तक में मूल बातों में कमी लाने की जहमत नहीं उठाई क्योंकि यह 20,000 पृष्ठों की लंबी होती और डराती हुई आपको वहीं पर रैक से दूर कर देती है जब तक आप इसे उठा नहीं लेते। इसके बजाय, मैं चाहता हूं कि आप पहले "101" सामान सीखें ताकि आप इस पुस्तक के साथ सफल हो सकें।

यह लंबा नहीं लगेगा, और यह रॉकेट साइंस नहीं है। मुझे अलबामा के पब्लिक स्कूल सिस्टम में शिक्षित किया गया था और पता नहीं था कि केबल टीवी या वीसीआर का क्या मतलब है जब तक कि मैं लगभग एक किशोर नहीं था, और मैंने यह पता लगा लिया– आपके लिए यह कितना मुश्किल हो सकता है? शुरुआत के लिए यहां बहुत कुछ है, हालांकि, मुझ पर भरोसा करें। मैंने इसे उसी तरीके से लिखा, जो मैंने इसे सीखा: सरल, आसान और आदर्श रूप से मजेदार। यह सामान जरूरी नहीं है; आप बस पहले रास्ते से बाहर मूल बातें की जरूरत है। मुझे लगता है कि आप अपने लक्ष्यों के लिए एकदम सही हैं।

आप में से उन लोगों के लिए जो पहले से ही अपना समय लगा चुके हैं और मूल बातें जानते हैं, मुझे लगता है कि आप इस पुस्तक को सुखद आश्चर्यचकित करेंगे। आप स्पष्ट रूप से अब तक जानते हैं कि तकनीक जादू नहीं है, और न ही यह समझने के लिए जरूरी है कि यह कठिन है या कठिन है – यह सिर्फ यह सीख रहा है कि कुछ कैसे काम करता है ताकि आप इसे अपने लाभ के लिए उपयोग कर सकें। मैंने इस तरीके से एथिकल हैकिंग पर हमला करने की कोशिश की, जिससे चीजें संभव हो सकें और रास्ते में थोड़ी हंसी आए। लेकिन कृपया पूर्वाभास करें: आप इस पुस्तक को पढ़कर केवल इस Exam को पास नहीं कर सकते हैं और न ही करना चाहिए। कोई भी किताब जो आपसे वादा करती है कि आपसे झूठ बोल रही है। हाथों के प्रयासों के बिना, बहुत सारे अभ्यास, और

अतिरिक्त अध्ययन के एक पूरे, आप बस सफल नहीं होंगे। इस पुस्तक को कुछ हाथों के अभ्यास के साथ मिलाएं, और मुझे नहीं लगता कि आपको Exam में कोई परेशानी होगी। प्रमाणीकरण के लिए इसे वन–स्टॉप–शॉप के रूप में पढ़ें, हालांकि, और आप Exam कक्ष को छोड़कर सोचेंगे कि आपके साथ क्या हुआ है।

निश्चित रूप से, इस पुस्तक का एक प्राथमिक लक्ष्य और ध्यान केंद्रित है – Version 10 Exam उत्तीर्ण करके आपको प्रमाणित एथिकल हैकर का खिताब हासिल करने में मदद करना। मेरा मानना है कि यह पुस्तक आपको वह सब कुछ प्रदान करती है, जिसकी आपको Exam उत्तीर्ण करनी होगी। हालाँकि, मुझे लगता है कि यह उससे कहीं अधिक है। मुझे आशा है कि मैं एक अन्य लक्ष्य में भी सफल हुआ जो कि उतना ही महत्वपूर्ण है: वास्तव में एक नियोजित नैतिक हैकर बनने में आपकी मदद करना। नहीं, ऐसा कोई तरीका नहीं है कि कोई व्यक्ति बस एक किताब उठा सकता है और जादुई रूप से इसे पढ़कर सिर्फ एक अनुभवी आईटी सुरक्षा पेशेवर बन सकता है, लेकिन मुझे पूरी उम्मीद है कि मैंने पर्याप्त वास्तविक–विश्व अंतर्दृष्टि प्रदान की है, जिस पर आप इस पुस्तक को सुरक्षित रूप से रखने पर भरोसा कर सकते हैं वास्तविक दुनिया में आपकी यात्रा।

How to Use This Book

इस पुस्तक के बारे में बात करते हुए, इसमें वह सब कुछ शामिल है जो आपको ईसीसीएल के प्रमाणित एथिकल हैकर Exam के लिए जानना होगा। प्रत्येक अध्याय ईसी–काउंसिल द्वारा परिभाषित Exam के लिए विशिष्ट उद्देश्यों और विवरणों को शामिल करता है। मैंने उन्हें पूरी तरह से व्यवस्थित करने की पूरी कोशिश की है, जो मुझे समझ में आता है, और मुझे आशा है कि आप इसे उसी तरह से देखेंगे।

प्रत्येक अध्याय में कई घटक हैं जो आपको Exam के लिए आवश्यक जानकारी को प्रभावी ढंग से बताने के लिए डिज़ाइन किए गए हैं:

- प्रत्येक अध्याय में शामिल प्रमाणीकरण उद्देश्यों को पहले सूचीबद्ध किया गया है, ठीक बल्ले से। ये अध्याय के भीतर प्रमुख विषयों की पहचान करते हैं और आपको अपने अध्ययन का नक्शा बनाने में मदद करते हैं।

- साइडबार को प्रत्येक अध्याय में शामिल किया गया है और इसे सूचनाओं, युक्तियों और कहानियों को इंगित करने के लिए डिज़ाइन किया गया है जो आपकी दिन–प्रतिदिन की जिम्मेदारियों में सहायक होंगे। उल्लेख नहीं करने के लिए, वे कभी–कभी मज़ाक उड़ाते हैं।

  कृपया ध्यान दें, हालांकि, हालांकि ये प्रविष्टियाँ वास्तविक दुनिया की जानकारी के दिलचस्प अंश प्रदान करती हैं, लेकिन कभी–कभी इन्हें परीक्षण योग्य सामग्री को सुदृढ़ करने के लिए उपयोग किया जाता है। केवल उन्हें "स्वच्छ" के रूप में छूट न दें परिस्थितियों और इन साइडबार में वर्णित औजारों की सही–सही Exam में एक प्रश्न या दो का उत्तर देने में अंतर साबित हो सकता है।

- Exam युक्तियाँ ठीक वही हैं जो वे पसंद करते हैं। इनमें शामिल हैं उस क्षेत्र को इंगित करें जहां आपको Exam के लिए ध्यान केंद्रित करने की आवश्यकता है। नहीं वे हैं स्पष्ट परीक्षण उत्तर नहीं। हां, वे आपके अध्ययन पर ध्यान केंद्रित करने में आपकी मदद करेंगे।

- विशेष रूप से कहे जाने वाले नोट्स भी प्रत्येक अध्याय का हिस्सा हैं। ये जानकारी के दिलचस्प हैं जो चर्चा के लिए प्रासंगिक हैं और अतिरिक्त जानकारी को इंगित करते हैं। साइडबार के साथ ही, उन्हें छूट न दें।

The Examination

इससे पहले कि मैं कुछ और करूं, मुझे स्पष्ट होने दें: यह पुस्तक आपको अपना परीक्षण पास करने में मदद करेगी। मैंने यह सुनिश्चित करने के लिए महान दर्द उठाया है कि ईसी–काउंसिल ने आपको पुस्तक में शामिल होने से पहले जानने के लिए कहा है, और मुझे लगता है कि यह बहुत अच्छी तरह से कवर किया गया है। फिर से, मेरे पास एक सावधानी का नोट है जिसे मैं यहां रखना चाहता हूं, और वह इस पुस्तक को अध्ययन के एकमात्र स्रोत के रूप में उपयोग नहीं करता है। यह सलाह किसी भी पुस्तक के लिए किसी भी प्रमाणन के लिए जाती है। आप बस एक पुस्तक लेने और एक प्रमाणीकरण Exam पास करने की उम्मीद नहीं कर सकते। आपको अभ्यास की आवश्यकता है। आपको हाथों के अनुभव की आवश्यकता है, और आपको कुछ और अभ्यास करने की आवश्यकता है। और कोई भी – किसी भी प्रकाशक, लेखक, या स्थानीय स्टोर में एक लंबी पारी के माध्यम से मित्रवत पुस्तक बिक्री लिपिक भाग–जो कहता है कि अन्यथा उनके दांतों के माध्यम से झूठ बोल रहा है।

हां, मुझे पूरा विश्वास है कि यह पुस्तक शुरू करने के लिए एक शानदार जगह है और आपके अध्ययन का मार्गदर्शन करने का एक अच्छा तरीका है। बस अजीब अति आत्मविश्वास के साथ इस Exam में न जाएं क्योंकि "मैं किताब पढ़ता हूं इसलिए मैं अच्छा हूं।" Exam अक्सर बदलती रहती है, जैसा कि यह होना चाहिए, और नई सामग्री पतली हवा से बाहर निकलती है जैसे दिन बीतते हैं। अपने आप को उन सभी चीज़ों के बारे में बताएं जो आप अपने हाथों से प्राप्त कर सकते हैं, और अच्छाई की खातिर एक होम लैब का निर्माण करते हैं और कुछ (बहुत सारे) हाथों से साधना शुरू करते हैं। अनुभव के लिए कोई विकल्प नहीं है, और मैं आपसे वादा करता हूं, Exam का समय आएगा, आपको खुशी होगी कि आपने अपना समय अंदर डाल दिया।

परीक्षण की बात करते हुए (आधिकारिक तौर पर सीईएच 312–50, Version 10 इस लेखन के रूप में), यह कौशल और नौकरी–भूमिकाओं के आधार पर सीखने, मानक–आधारित प्रशिक्षण मॉड्यूल और बेहतर उद्योग स्वीकृति प्रदान करने के लिए डिज़ाइन किया गया था। –आर्ट लैब (सरकारी कोर्सवेयर और ऑनलाइन में)। Exam में 125 बहुविकल्पीय प्रश्न होते हैं और 4 घंटे तक रहते हैं। एक उत्तीर्ण अंक 70 प्रतिशत है (दूसरे शब्दों में, आपको कम से कम 88 प्रश्न सही होने चाहिए)। वितरण VUE और ECC द्वारा प्रदान किया जाता है।

इन tidbits आपकी मदद करनी चाहिए:

- अध्यायों में Exam के सुझावों पर पूरा ध्यान देना सुनिश्चित करें। वे वहां किसी कारण की वजह से हैं। और Examओं को फिर से लिखें– दोनों अध्याय की Exam और इलेक्ट्रॉनिक Exam – जब तक आप उनमें से बीमार न हों। वे मेरी मदद

करेंगे, मुझ पर भरोसा करेंगे।

- आपको बाद में समीक्षा के लिए प्रश्नों को चिह्नित करने और छोड़ने की अनुमति है। पूरी Exam से गुज़रें, जिनका उत्तर आप जानते हैं कि आप संदेह की छाया से परे हैं। जिन लोगों के बारे में आप निश्चित नहीं हैं, वैसे भी एक उत्तर चुनें और आगे की समीक्षा के लिए प्रश्न को चिह्नित करें (आप Exam में असफल नहीं होना चाहते हैं क्योंकि आप समय से बाहर भाग गए थे और प्रश्नों का एक गुच्छा था जो एक भी नहीं था उत्तर चुना)। प्रत्येक अनुभाग के अंत में, वापस जाएं और उन लोगों को देखें जिन्हें आपने चिह्नित किया है। अपना उत्तर तभी बदलें, जब आप पूरी तरह से इसके बारे में 100 प्रतिशत निश्चित हों।

- आप पूर्ण निश्चितता के साथ, कुछ type के प्रश्न देखेंगे, जो आपके दिमाग को उड़ा देंगे। एक या दो बाएं क्षेत्र से पूरी तरह से बाहर आ जाएंगे। मैंने CEH Exam छह बार ली है – Version 5 से वर्तमान Version 9 तक (जो कि इस पुस्तक के लिए लिखा गया है) – और हर बार जब मैंने ऐसे प्रश्न देखे हैं जो लग रहे थे कि मुझे अभी तक यकीन नहीं हुआ था सही Exam ले रहा था। जब आप उन्हें देखते हैं, तो घबराएं नहीं। डिडक्टिव रीजनिंग का उपयोग करें और अपना सर्वश्रेष्ठ अनुमान लगाएं। इस Exam के लगभग हर एक प्रश्न का अनुमान एक अनुमान के अनुसार कम से कम 50/50 बाधाओं पर लगाया जा सकता है। दूसरे type के प्रश्न जो आप देखेंगे, जिससे आपको लगता है कि प्रश्न वास्तविकता वास्तविकता अंग्रेजी भाषा के संबंध में बहुत खराब व्याकरण का उपयोग करेगा। बस याद रखें कि यह एक अंतरराष्ट्रीय

संगठन है और कभी–कभी चीजें आसानी से अनुवाद नहीं करती हैं।

- Exam के कोड प्रश्नों पर (जहां कोड स्निपेट आपके लिए सवालों के जवाब देने के लिए दिखाए गए हैं), पोर्ट संख्याओं पर ध्यान दें। यहां तक कि अगर आप लॉग या कोड उत्पन्न करने के बारे में अनिश्चित हैं, तो आप आमतौर पर पोर्ट नंबर को बहुत जल्दी से देख सकते हैं। यह निश्चित रूप से एक या दो सवाल पर आपकी मदद करेगा। इसके अतिरिक्त, कोड स्निपेट के दाईं ओर सादे पाठ की उपेक्षा न करें। यह अक्सर आपको दिखा सकता है कि उत्तर क्या है।

Domains

परीक्षण युक्तियों के अलावा और प्रमाणित कैसे प्राप्त करें, सबसे अधिक बार पूछे जाने वाले प्रश्नों में से एक है, "हे मैट, परीक्षण में क्या है?" असंख्य कारणों पर ध्यान देने के बाद कि मैं सटीक परीक्षण प्रश्न और उत्तर (नैतिकता और नॉनडिसक्लोजर एग्रीमेंट और ऐसे) प्रदान नहीं कर सकता हूं, मैं आमतौर पर इस पुस्तक में सब कुछ के साथ जवाब देता हूं। और थोड़ा और।अब एमी स्टोनब्रोकर, मैकग्रा–हिल एजुकेशन के अधिग्रहण संपादक के लिए धन्यवाद, इस परियोजना पर मेरे साथ काम करने की अटूट खुशी के साथ दुख की बात है, और उसके ceaseless लेकिन ध्यान से गणना की और शानदार ढंग से निष्पादित योजना मुझे उसके हर विचार और विचार पर प्रस्तुत करने के लिए हरा दिया। पुस्तक, मैं उत्तर के रूप में इस छोटे से खंड में सभी को इंगित कर सकता हूं।

अब मुझे पता है कि आप में से कुछ इसे पढ़ रहे हैं और कह रहे हैं, "एक मिनट रुको.... यह एक ऑल–इन–वन अध्ययन गाइड माना जाता है।

वहाँ "और थोड़ा और" जोड़ के साथ आपका क्या मतलब है? मुझे लगा कि आपने इस पुस्तक में सब कुछ शामिल किया है? और एमी को यहाँ पर पाने के लिए आपको इतना पीटना क्यों पड़ा?" मुझे समझाने दो।

सबसे पहले, मैं एक त्वरित शिक्षार्थी हूं, और इस पुस्तक के पहले दो Version से समीक्षा और प्रतिक्रियाएं मुझे एक अकाट्य सत्य की ओर ले जाती हैं: कोई भी स्थिर पुस्तक जो कभी भी नहीं लिखी गई है, ईसी–काउंसिल उनकी Exam की कतार में फेंकने का फैसला करती है। प्रकाशन के कुछ महीने बाद, ईसी–काउंसिल अतीत से कुछ अयोग्य हमले के संबंध में या कुछ ऐसा हो सकता है जिसके बारे में सवाल करने का निर्णय ले सकती है (यानी, हार्दिक–शैली Vulnerability घोषणाएं)। यह सिर्फ प्रमाणन Examओं की प्रकृति है: इसमें से कुछ नया होने जा रहा है, कोई फर्क नहीं पड़ता कि आप किस प्रशिक्षण स्रोत का उपयोग करते हैं। और, हां, इसमें उनकी अपनी आधिकारिक पाठ्यक्रम सामग्री भी शामिल है।

दूसरा, और मैकग्रा–हिल एजुकेशन में संपादक–लेखक रिश्तों में अंतर्दृष्टि के अधिक दिलचस्प सवाल के लिए, एमी को मुझ पर काफी मार पड़ी क्योंकि हम इस पुस्तक में उद्देश्य के नक्शे शामिल करने पर असहमत थे। एमी ने सही उल्लेख किया कि एक उद्देश्य मानचित्र उम्मीदवारों को उनके अध्ययन पर ध्यान केंद्रित करने में मदद करता है और साथ ही प्रशिक्षकों को पाठ योजना और कक्षा कार्यक्रम बनाने में मदद करता है। मेरा तर्क तीन बातों पर केंद्रित था। सबसे पहले यह अपरिहार्य तथ्य है कि ईसी–काउंसिल के उद्देश्यों को स्पष्ट रूप से कहा जा सकता है, और अक्सर आप यह नहीं पा सकते हैं कि आप उनके बारे में क्या जानना चाहते हैं या उनके आधिकारिक शोध में ज्ञान का परीक्षण किस स्तर तक किया जाएगा। दूसरा, उद्देश्यों को

केवल ईसी–काउंसिल के आधिकारिक कोर्सवेयर में ही पाया जा सकता है (आप उनकी वेबसाइट पर एक परीक्षण ब्रेकडाउन और ऐसे पा सकते हैं, लेकिन अब उद्देश्य नहीं) और उस से कॉपी / पेस्ट करना एक नहीं–नहीं है। तीसरा, ईसी–काउंसिल पूरी तरह से Version से दूर जा रहा है और निरंतर व्यावसायिक शिक्षा मॉडल को अपना रहा है जो कि अन्य प्रमाणन प्रदाता उपयोग करते हैं। इसका मतलब है, प्रिय पाठक, ईसी–काउंसिल किसी भी समय अपने उद्देश्यों को बदल सकता है और बदल सकता है, जैसा कि वे महसूस करते हैं कि यह दूसरे संस्करण को जारी करता है। "

तो, एक पहेली – जो एमी ने हमारे लिए हल किया क्योंकि वह सिर्फ उस तरह से भयानक है। हम आपके लिए प्रस्तुत हैं] प्रिय पाठक, इस पुस्तक के लिए एक डोमेन मैप के साथ। ईसी–काउंसिल अपने वर्तमान (और भविष्य) CEH प्रमाणीकरण के लिए 18 डोमेन को परिभाषित करता है। हमने आपके उपयोग के लिए इन डोमेन को अध्यायों में मैप कर दिया है:

	CEH Exam 312-50
CEHv9 Core Modules	**All-in-One Coverage**
Introduction to Ethical Hacking	Chapter 1: Getting Started: Essential Knowledge
Footprinting and Reconnaissance	Chapter 2: Reconnaissance: Information Gathering for the Ethical Hacker
Scanning Networks	Chapter 3: Scanning and Enumeration
Enumeration	Chapter 3: Scanning and Enumeration
System Hacking	Chapter 5: Attacking a System
Malware Threats	Chapter 9: Trojans and Other Attacks
Evading IDS, Firewalls and Honeypots	Chapter 4: Sniffing and Evasion
Sniffing	Chapter 4: Sniffing and Evasion
Social Engineering	Chapter 11: Low Tech: Social Engineering and Physical Security
Denial of Service	Chapter 9: Trojans and Other Attacks
Session Hijacking	Chapter 9: Trojans and Other Attacks
Hacking Webservers	Chapter 6: Web-Based Hacking: Servers and Applications
Hacking Web Applications	Chapter 6: Web-Based Hacking: Servers and Applications
SQL Injection	Chapter 6: Web-Based Hacking: Servers and Applications
Hacking Wireless Networks	Chapter 7: Wireless Network Hacking
Hacking Mobile Platforms	Chapter 7: Wireless Network Hacking
Cloud Computing	Chapter 8: Security in Cloud Computing
Cryptography	Chapter 10: Cryptography 101

तो वहाँ आपके पास है, महिलाओं और सज्जनों। उम्मीद है कि यह आपके अध्ययन / कक्षा को तैयार करने में मदद करता है और किसी भी आशंका को शांत करता है जिसे हमने कुछ छोड़ दिया है।

The Certification

तो, आपने अध्ययन किया है, आप पहले से तैयार हैं, और आपको लगता है कि आप CEH प्रमाणित बनने के लिए तैयार हैं। आमतौर पर इस प्रमाण पत्र की तलाश करने वाले अधिकांश लोगों का मानना है कि उनका अगला कदम बस एक Exam लेने के लिए है, और सालों तक (जैसा कि ज्यादातर अन्य प्रमाणपत्रों के लिए मामला है) यह सच्चाई थी। हालांकि, समय में बदलाव, और प्रमाणन प्रदाता

हमेशा अपने शीर्षक के लिए अधिक मूल्य जोड़ने के लिए एक रास्ता तलाश रहे हैं। ईसी–काउंसिल अलग नहीं है, और इसने उम्मीदवारों के लिए चीजों को थोड़ा बदल दिया ळें

जब आप प्रमाणन के लिए आवेदन करते हैं, तो कुछ चीजें होती हैं जिन्हें ईसीसी कार्यक्रम की अखंडता की रक्षा करने के लिए कहता है। पहला एक हस्ताक्षरित अनुबंध है जिसके तहत आप शरारती उद्देश्यों के लिए प्रदान किए गए ज्ञान का उपयोग नहीं करने का वादा करते हैं: इस पाठ्यक्रम में भाग लेने से पहले, आपको यह कहते हुए एक समझौते पर हस्ताक्षर करने के लिए कहा जाएगा कि आप अवैध या दुर्भावनापूर्ण हमलों के लिए नए अधिग्रहीत कौशल का उपयोग नहीं करेंगे और आप किसी भी कंप्यूटर प्रणाली से समझौता करने के प्रयास में ऐसे उपकरण का उपयोग न करें, और इन उपकरणों के उपयोग या दुरुपयोग के संबंध में ईसी–परिषद की निंदा करने के इरादे की परवाह किए बिना। दूसरा यह है कि आप इस बिरादरी में होने के लिए सत्यापन के कुछ type हैं – यानी, आप यह जानने के लिए काफी समय से काम कर रहे हैं कि आप क्या कर रहे हैं, या यह कि आपने उपयुक्त प्रशिक्षण पूरा कर लिया है (ईसी की नजर में– वैसे भी परिषद) उस के लिए बनाने के लिए।

CEH प्रमाणन प्राप्त करने के लिए एक उम्मीदवार के लिए दो तरीके हैं: प्रशिक्षण के साथ या केवल स्व–अध्ययन का उपयोग करना। प्रशिक्षण का विकल्प बहुत सीधा है: Exam का प्रयास करने से पहले आपको एक अनुमोदित CEH प्रशिक्षण वर्ग में भाग लेना चाहिए। और वे वास्तव में, वास्तव में, वास्तव में चाहते हैं कि आप उनके प्रशिक्षण वर्ग में भाग लें। प्रति साइट (http://iclass.eccouncil.org/?p=719), प्रशिक्षण के विकल्पों में निम्नलिखित शामिल हैं:

- **Live, Online Instructor-Led** –लेड ये कई प्रशिक्षण सहयोगियों द्वारा दिए जाते हैं ईसी–काउंसिल ने प्रशिक्षण प्रदान करने के लिए प्रमाणित किया है। वे दो तरीकों में से एक में आधिकारिक कोर्सवेयर प्रदान करते हैं: एक मानक कक्षा सेटिंग या "ऑनलाइन–लाइव" प्रशिक्षण वर्ग के माध्यम से आप कहीं से भी देख सकते हैं। दोनों प्रसादों में एक ECC प्रमाणित प्रशिक्षक होता है और इस लेखन में $2,895 प्रति सीट खर्च होता है।

- **Client-Site** –काउंसिल आपके स्थान पर एक वर्ग के लिए भी व्यवस्था कर सकती है, बशर्ते आप इसके लिए भुगतान करने के इच्छुक हों, बेशक। उसके लिए लागत आपके संगठन पर निर्भर करती है।

इसे अपने दम पर करने के लिए, कुछ तरीके उपलब्ध हैं:

- **I-Learn -** इस विकल्प में, आप क्लास के लिए उपयोग की जाने वाली प्रयोगशालाओं के साथ–साथ आधिकारिक कोर्सवेयर और प्रीएकॉर्डेड प्रसाद का भुगतान करते हैं। यह आपको अपने दम पर सामान के माध्यम से काम करने की अनुमति देता है, बिना प्रशिक्षक। इस लेखन की लागत $1,899 है,

- **Self-Study -** आप जो पहले से जानते हैं), आप केवल $ 870 के लिए कोर्सवेयर खरीद सकते हैं और अपने दम पर अध्ययन कर सकते हैं।

एक बार जब आप प्रशिक्षण में भाग लेते हैं, तो आप Exam के लिए

पंजीकरण कर सकते हैं और बिना किसी अतिरिक्त लागत या चरणों के Exam का प्रयास कर सकते हैं। तथ्य की बात के रूप में, Exam के लिए लागत आमतौर पर पाठ्यक्रम मूल्य निर्धारण का हिस्सा है। यदि आप स्व–अध्ययन का प्रयास करते हैं, हालांकि, कुछ अतिरिक्त आवश्यकताएं हैं, यहां विस्तृत, सीधे ईसी–काउंसिल से।

आधिकारिक प्रशिक्षण में भाग लेने के बिना ईसी–काउंसिल प्रमाणन Exam के लिए विचार करने के लिए, उम्मीदवार को होना चाहिए:

- कम से कम दो साल की सूचना सुरक्षा–संबंधित अनुभव है।
- USD100 के एक अकाट्य पात्रता आवेदन शुल्क को हटाएं।
- एक पूर्ण Exam पात्रता आवेदन पत्र जमा करें। (आवेदक को https://cert.eccouncil.org/exam-eligibility-form.html पात्रता आवेदन पत्र के लिए एक ऑनलाइन अनुरोध भरने के लिए। यूएसए /कनाडा के आवेदक एप्लिकेशंस pplicationservices@eccouncil.org,से संपर्क कर सकते हैं। और अंतर्राष्ट्रीय आवेदक cehapp@eccouncil.org से संपर्क कर सकते हैं। ईसी–काउंसिल आवेदक के बॉस / पर्यवेक्षक / विभाग प्रमुख से संपर्क करेगा, जो प्रमाणीकरण प्रयोजनों के लिए आवेदन पत्र में आवेदक के सत्यापनकर्ता के रूप में कार्य करने के लिए सहमत हो गया है। यदि आवेदन को मंजूरी दी जाती है, तो आवेदक को ईसी–काउंसिल से सीधे वाउचर खरीदना आवश्यक होगा। ईसी–काउंसिल तब उम्मीदवार को पात्रता कोड और वाउचर कोड भेजेगा, जिसका उपयोग उम्मीदवार विश्व स्तर पर किसी भी अधिकृत VUE परीक्षण केंद्र में परीक्षण को पंजीकृत करने और निर्धारित करने के लिए कर सकते हैं। कृपया ध्यान दें कि VUE पंजीकरण पात्रता कोड के बिना किसी भी अनुरोध का मनोरंजन नहीं

करेगा। यदि आवेदन स्वीकृत नहीं हुआ है, तो USD100 का आवेदन शुल्क वापस नहीं किया जाएगा।)

- http://store.eccouncil.org/ स्टोर के माध्यम से ईसी–काउंसिल से सीधे एक आधिकारिक Exam वाउचर खरीदें।

और वहाँ आपके पास है, प्रिय पाठक। निश्चित रूप से, स्व–अध्ययन का उपयोग करके सीईएच के लिए कूदने के लिए अतिरिक्त हुप्स के एक जोड़े हैं, लेकिन यह सबसे अच्छा विकल्प है, लागत–वार। किसी ऐसे व्यक्ति के दृष्टिकोण से, जिसने सुरक्षा दुनिया में कई कर्मचारियों को काम पर रखा है, मेरा मानना है कि यह चारों ओर से बेहतर विकल्प हो सकता है: कोई भी एक वर्ग में शामिल हो सकता है, लेकिन स्व–अध्ययन करने वालों को यह सत्यापित करने के लिए एक प्रायोजक की आवश्यकता है कि उनके पास उपयुक्त है अनुभव। मेरी विनम्र राय में यह अतिरिक्त कदम के लायक है।

अंत में, इस पुस्तक को लेने के लिए धन्यवाद। मुझे पूरी उम्मीद है कि आपकी Exam अच्छी तरह से होगी, और मैं आपको आपके आगामी करियर में पूर्ण रूप से शुभकामनाएं देता हूं। यहाँ उम्मीद है कि मैं तुम्हें वहाँ देख रहा हूँ, कहीं और कभी!

CHAPTER 1

GETTING STARTED

मैं इसे आपके और आपके अध्ययन के लिए बेहतर रूप से केंद्रित रखने के लिए अपना सर्वश्रेष्ठ प्रदर्शन करने जा रहा हूं। इस अध्याय में अभी भी कुछ असमान रूप से उबाऊ और सांसारिक जानकारी शामिल है जो संभवतः उस कपड़े धोने के रूप में रोमांचक है जिसे आपने मशीन में जाने के लिए इंतजार कर ढेर कर दिया है, लेकिन यह कहा जाना है, और आप इसे सुनने वाले हैं। हम कई शब्दों को शामिल करेंगे जिन्हें आपको जानना होगा, जिसमें एक एथिकल हैकर भी शामिल है, और हो सकता है कि आप उन दो चीजों को भी कवर करें जिन्हें आप नहीं जानते हैं।

Security

यदि आप एक नैतिक हैकिंग प्रमाणीकरण की ओर एक यात्रा शुरू करने जा रहे हैं, तो यह पालन करना चाहिए कि सुरक्षा के साथ शामिल मूलभूत परिभाषाएं और शब्दावली प्रारंभिक रेखा पर सही होनी चाहिए। हम यहां आईटी सुरक्षा में शामिल हर चीज को कवर नहीं करने जा रहे हैं – यह बस एक विषय है, हमारे पास जगह नहीं है, और आपको वैसे भी हर तत्व पर परीक्षण नहीं किया जाएगा – लेकिन 101–स्तरीय ज्ञान की एक नींव है आपके पास उथले सिरे से बाहर निकलने से पहले होना चाहिए। इस अध्याय में उन शब्दों को शामिल किया गया है, जिनकी आपको अन्य लोगों के साथ सुरक्षा मामलों पर चर्चा करते समय बुद्धिमानी से जानने की आवश्यकता होगी। और, शायद उतने ही महत्वपूर्ण, हम टीसीपी / आईपी नेटवर्किंग के कुछ मूल बातें कवर करेंगे, क्योंकि आखिरकार, अगर आप भाषा नहीं समझते हैं, तो आप बातचीत में अपना काम कैसे करेंगे?

Essentials

इससे पहले कि हम यह जान सकें कि एक हैकर क्या है और आप हमारे विषय के विषय के माध्यम से हमारे रोम–रोम में कैसे एक हो जाते हैं, कुछ चीजें हैं, जिनसे मुझे बाहर निकलने की जरूरत है। सबसे पहले, भले ही मैंने किताब के लिए उस शेक्सपियरन परिचय में यह सबसे अधिक कवर किया हो, मैं इस Exam के बारे में थोड़ी बात करना चाहता हूं और आपको इसे जानने के लिए, और करने की आवश्यकता है। खुद को क्यों दोहराएं? क्योंकि हमारे पहले कुछ आउटिंग से समीक्षाओं, टिप्पणियों और ई–मेल को पढ़ने के बाद, यह मेरे ध्यान में आया है कि आप में से कोई भी वास्तव में परिचय नहीं पढ़ता है। मैं तुम्हें दोष नहीं देता; मैं इसे ज्यादातर सर्टिफिकेशन स्टडी बुक्स पर छोड़ देता हूं, सिर्फ मीट के लिए ही सही। लेकिन वहाँ अच्छी चीजें हैं जो आपको आगे पढ़ने से पहले वास्तव में जानने की आवश्यकता है, इसलिए मैं आपके सामने सामने आने के लिए एक त्वरित ठहरनेवाला काम करूंगा।

दूसरा, हमें कुछ सुरक्षा और नेटवर्क बेसिक्स को कवर करने की आवश्यकता है जो आपकी Exam में मदद करेंगे। इस खंड में से कुछ बस बुनियादी याद है, इसमें से कुछ सही सामान्य ज्ञान है, और कुछ यह है, या होना चाहिए। आप वास्तव में यह पहले से ही जानने वाले हैं, और आप इस सामान को इस पुस्तक में बार–बार देखेंगे, लेकिन यह वास्तव में आधारभूत सामान है और यदि मैं कम से कम एक जंपिंग–पॉइंट प्रदान नहीं करता तो मुझे रिमिस होगा।

The Exam

क्या आप नीचे बैठे हैं? क्या आपका दिल स्वस्थ है? मैं आपको इस चौंकाने वाले रहस्योद्घाटन से परेशान नहीं करना चाहता। तुम तैयार हो? सीईएच Version 10 Exam मुश्किल है, और अध्ययन और कई अध्ययन स्रोतों के घंटे (दिन, सप्ताह) के बावजूद, आप अभी भी

Exam के एक Version में आ सकते हैं जो आपको महसूस कर रहा है कि आप एक ट्रक से टकरा गए हैं।

मुझे पता है। एक आदमी ने एक स्टडी बुक लिखी और बेची, बस आपको बता दिया कि यह पर्याप्त नहीं होगा। जब मैं कहूं तो मुझ पर विश्वास करो, हालांकि, मैं मजाक नहीं कर रहा हूं। बेशक यह एक अच्छा अध्ययन संदर्भ होगा। यदि आप वास्तव में चाहते हैं तो बेशक आप इससे कुछ सीख सकते हैं। निश्चित रूप से मैंने सब कुछ किया जो मैं इसे संभव के रूप में अद्यतित और व्यापक बना सकता हूं। लेकिन अगर आप पागल धारणा के तहत हैं तो यह एक जादू का टिकट है, कि 2016 से किसी भी तरह से लिखा गया शब्द एक विशिष्ट परीक्षण प्रश्न पर शब्द–दर–शब्द संदर्भ को जादुई रूप से हिट करने वाला है जो आप इसे पढ़ रहे हैं।

ईमानदारी से आपको कुछ पेशेवर मदद पाने के लिए प्रोत्साहित करें इससे पहले कि फर्नीचर आपसे बात करना शुरू कर दे और बिल्ली समझ में आने लगे। आप में से जो सटीक Exam के प्रश्नों की तलाश कर रहे हैं और Exam में उत्तीर्ण होने के लिए रटे–रटे संस्मरण इस प्रकाशन में नहीं पाएंगे, न ही कोई अन्य। आप में से बाकी लोगों के लिए, जो Exam के लिए सही तरीके से तैयारी करने के लिए थोड़ा ध्यान केंद्रित करना चाहते हैं और जो लोग यह जानना चाहते हैं कि वास्तव में एक नैतिक हैकर होने का क्या मतलब है, आइए अपने परीक्षण की मूल बातों के साथ चलें।

नोट - मुझे पूछा गया है, बहुत कुछ, Version 7 और Version 10 के बीच क्या अंतर है, और जवाब है, वास्तव में, बहुत ज्यादा नहीं। ईसीसी ने बफर ओवरफ्लो पर अध्याय को हटा दिया (लेकिन इसे वेब हमलों में एक संदर्भ के रूप में छोड़ दिया), सभी चीजों को मोबाइल

का विस्तार किया, और क्लाउड कंप्यूटिंग पर एक नया खंड जोड़ा। वे भी पूरी तरह से आगे बढ़ते हुए Version करण से मुक्त हो गए, एक सतत शिक्षा मॉडल पर अधिक जा रहे थे। अन्यथा, नेटवर्किंग अभी भी नेटवर्किंग है, और पिछले Version के लिए आपके द्वारा अध्ययन किया गया सामान यहां लागू होगा।

सबसे पहले, यदि आपने कभी प्रमाणन–स्तर की Exam नहीं ली है, तो मैं इसे आपके कुंवारी अनुभव के रूप में नहीं सुझाऊँगा। आपके पहले वॉकथ्रू में शामिल सभी विकर्षणों और तंत्रिकाओं के बिना यह काफी कठिन है। जब आप अपनी Exam के लिए आते हैं, तो आप आमतौर पर एक दोस्ताना टेस्ट प्रॉक्टर या रिसेप्शनिस्ट के साथ जांच करते हैं, कुछ चीजों पर हस्ताक्षर करते हैं, और अपने परीक्षण कक्ष में फ़नल हो जाते हैं। जब भी मैं गया हूँ हर बार यह एक छोटा कार्यालय या एक बंद कक्ष रहा है, जिसमें एक एकल मॉनीटर आपको अचरज से देखता है।

आप START पर क्लिक करेंगे और एक–एक करके प्रश्नों के माध्यम से व्हिस्ज़िंग करना शुरू करेंगे, सबसे अच्छे उत्तर का चयन करने के लिए मंडली पर क्लिक करके या सही खंड पर परिभाषाएँ क्लिक करके और खींचकर। इसके अंत में एक SUBMIT बटन है, जिसे आप क्लिक करेंगे और फिर समय–स्थान सातत्य में एक ब्रेक दर्ज करेंगे– क्योंकि अगले 10 सेकंड आपके जीवन के सबसे लंबे समय तक लगेंगे। वास्तव में, यह एक अनंत काल की तरह प्रतीत होगा, जहाँ चीजें बहुत धीमी हो गई हैं, आप वास्तव में मॉनिटर पर ताज़ा दर देख सकते हैं और कार्यालय लैंप के माध्यम से बहने वाले एसी करंट के चक्रों को नोटिस कर सकते हैं। जब परिणाम पृष्ठ अंतिम रूप से प्रकट होता है, तो यह अत्यधिक राहत या एक वास्तविक सुन्नता का क्षण होता है।

यदि आप पास करते हैं, तो अध्ययन सामग्री में से कोई भी मायने नहीं रखता है और स्पष्ट रूप से, आप लगभग तुरंत अपने न्यूरॉन्स से संग्रहीत मेमोरी को डंप करना शुरू कर देंगे। यदि आप पास नहीं करते हैं, तो सब कुछ मायने रखता है। आप कार की दौड़ करेंगे और जो कुछ भी आप याद कर सकते हैं उसे शुरू करना है ताकि आप अगली बार बेहतर अध्ययन कर सकें। आप सोशल मीडिया और इंटरनेट पर चर्चा करने के लिए उड़ान भरेंगे कि क्या गलत हुआ और किसी भी चीज को तैयार करने के लिए जो आपको तैयारी में उपयोगी नहीं लगी। और आप लगभग निश्चित रूप से कुछ के लिए देखेंगे, किसी को दोष देना। मेरा विश्वास करो, यह मत करो।

इस Exam की तैयारी में आप जो कुछ भी करते हैं वह आपको एक बेहतर एथिकल हैकर बनाने के लिए किया जाना चाहिए, न कि किसी Exam में पास होने के लिए। यदि आप इस तरह से तैयारी करते हैं जैसे कि यह आपका काम है, यदि आप अध्ययन सामग्री के लिए उपयोग की जाने वाली सभी चीजों को लेते हैं और याद रखने के बजाय सीखने की कोशिश करते हैं, तो आप बेहतर बंद, पास या असफल होंगे। और, फलस्वरूप, मैं गारंटी देता हूं कि यदि आप इस तरह से Exam के किसी भी Version को पास करने की अपनी योग्यता को तैयार करते हैं जो कि खगोलीय रूप से ऊपर जाती है।

परीक्षण ही? खैर, कुछ टिप्स और ट्रिक्स हैं जो मदद कर सकते हैं। मैं आपको सलाह देता हूं कि आप "Exam" और "प्रमाणीकरण" खंडों को पढ़ें। वे आपकी मदद करेंगे।बहुत। यहां कुछ अन्य युक्तियां दी गई हैं जो मदद कर सकती हैं:

- वास्तविक जीवन को ट्रम्प ईसी–काउंसिल के दृष्टिकोण से न जाने दें। आपके अध्ययन और अंतिम Exam के जीवन में कहीं न कहीं कई उदाहरण होंगे जहां आप कहेंगे, “वास्तव में

दुनिया में ऐसा नहीं होता है! किसी का दावा है कि एक लॉकर में भरवां किया जाएगा और शेविंग क्रीम के साथ सिर से पैर तक छिड़क दिया जाएगा!"जब मैं यह कहता हूं तो मुझ पर विश्वास करें: वास्तविक जीवन और एक प्रमाणन Exam जरूरी नहीं कि हमेशा सीधे आनुपातिक हो। इन सवालों में से कुछ पर, आपको अध्ययन करने और जानने की आवश्यकता होगी कि आपको Exam के लिए क्या चाहिए, यह अच्छी तरह से जानते हुए कि यह वास्तविक दुनिया में अलग है। यदि आपको नहीं पता कि मेरा इससे क्या मतलब है, तो किसी ऐसे व्यक्ति से पूछें जो कुछ समय से ऐसा कर रहा है यदि उन्हें लगता है कि सोशल इंजीनियरिंग निष्क्रिय है।

- अपने परीक्षण कक्ष में प्रवेश करने से पहले बाथरूम में जाएं। भले ही आपके पास नहीं है। क्योंकि, मुझ पर विश्वास करो, तुम करो।

- अपने लाभ के लिए समय का उपयोग करें। Exam अब खंडों में विभाजित है, जिसमें प्रत्येक के लिए एक समय सीमा निर्धारित है। आप अपने इच्छित अनुभाग के अंदर काम कर सकते हैं और समीक्षा कर सकते हैं, लेकिन एक बार जब आप इसके पास से गुजरते हैं तो आप वापस नहीं जा सकते। और यदि आप एक सेक्शन से उड़ान भरते हैं, तो आपको अगले एक पर अधिक समय नहीं मिलता है। अपना समय लें और उचित समीक्षा करें।

- ECC की वेबसाइट से, परीक्षण का टूटना निम्नानुसार है: पृष्ठभूमि पर 5 प्रश्न (नेटवर्किंग, प्रोटोकॉल, और इतने पर), विश्लेषण पर 16 / मूल्यांकन (जोखिम मूल्यांकन, तकनीकी

मूल्यांकन और डेटा का विश्लेषण), सुरक्षा पर 31 (सब कुछ) वायरलेस और सोशल इंजीनियरिंग से सिस्टम सुरक्षा नियंत्रण तक), उपकरण / सिस्टम / प्रोग्राम (उपकरण, सबनेटिंग, डीएनएस, एनएमएपी [40] पर 40...अहम], पोर्ट स्कैनिंग, और इतने पर), प्रक्रियाओं पर 25 (क्रिप्टोग्राफी, SOA, और इतने पर), विनियमन पर 5 (सुरक्षा नीतियों, अनुपालन) और नैतिकता पर 3 (मूल रूप से एक नैतिक हैकर बनाता है)। यदि वे वास्तव में उन मापदंडों के भीतर सब कुछ व्यवस्थित करेंगे, तो इससे बहुत मदद मिलेगी।

- कागज और पेंसिल / पेन का उपयोग करें जो मैत्रीपूर्ण परीक्षण प्रॉक्टर आपको प्रदान करता है। जैसे ही आप नीचे बैठते हैं, इससे पहले कि आप अशुभ परीक्षण मॉनिटर डिस्प्ले पर START क्लिक करें, प्रदान किए गए कागज पर अपने सिर से सब कुछ लिखना शुरू करें। आपको Exam केंद्र में चलने से ठीक पहले मैं समीक्षा करने की सलाह दूंगा कि जिन वर्गों की जानकारी आपको याद रखने में सबसे अधिक परेशानी हो रही है। जब आप अपने परीक्षण कक्ष में पहुंचें, तो उन्हें तुरंत लिख लें। इस तरह, जब आप Exam के माध्यम से अपने दिमाग को एक तिहाई से खो रहे हैं और घबराहट शुरू कर देते हैं कि आप याद नहीं कर सकते कि एक्सएमएएस एक closed port पर क्या रिटर्न देता है, तो आपके पास एक संदर्भ होगा। और मुझ पर विश्वास करो, वहां होने से आपको जानकारी को याद रखना आसान हो जाता है, भले ही आप इसे कभी न देखें।

- अपनी प्रकृति पर विश्वास रखें। जब आप प्रश्न समीक्षा करते हैं, जब तक कि आप बिल्कुल, सकारात्मक रूप से, संदेह के

किसी भी छाया से परे आपको पता है शुरू में गलत उत्तर को चिह्नित किया है, इसे बदलें नहीं।

- अंकित मूल्य पर प्रश्नों को लें। मैं ऐसे कई लोगों को जानता हूं जो ऐसा नहीं करते हैं Exam पर अच्छी तरह से क्योंकि वे पता लगाने की कोशिश कर रहे हैं कि परीक्षण लेखक क्या है मतलब जब सवाल एक साथ रखा। एक प्रश्न में मत पढ़ो; बस इसका जवाब दो और आगे बढ़ो।
- अपनी Exam को जितनी जल्दी हो सके, निर्धारित करें कि आप इसके लिए तैयार हैं। मैं ऐसा इसलिए कहता हूं क्योंकि मैं उन लोगों को जानता हूं जो कहते हैं, "मैं छह महीने के लिए अध्ययन करने जा रहा हूं और फिर मैं Exam देने के लिए तैयार रहूंगा।" छह महीने बीत जाते हैं और वे अभी भी वहां बैठे हैं, अध्ययन और तैयारी कर रहे हैं। यदि आप इसे कैलेंडर पर खुद को तैयार करने के लिए नहीं डालते हैं, तो आप इसे कभी नहीं लेंगे, क्योंकि आप कभी भी तैयार नहीं होंगे।

फिर, यह मेरा उद्देश्य है कि हर कोई इस पुस्तक को पढ़े और Exam की तैयारी में एक मूल्यवान संसाधन के रूप में इसका उपयोग करके प्रमाणन प्राप्त कर ले, लेकिन मैं आपको इसकी गारंटी नहीं दे सकता। क्योंकि, स्पष्ट रूप से, मैं आपको नहीं जानता। मुझे आपके काम की नैतिकता, विस्तार पर आपका ध्यान, या एक प्रमाणीकरण Exam प्रश्न से प्रभावी रूप से Exam और विवेकपूर्ण वास्तविकता लेने के लिए आपकी क्षमता को शांत करने की जानकारी नहीं है। मैं आपको केवल जानकारी प्रदान कर सकता हूं, आपको शुभकामनाएं देता हूं, और आपको ढीला कर देता हूं। अब, शो पर।

The OSI Reference Model

हम में से ज्यादातर ओएसआई संदर्भ मॉडल के बारे में सुनने के बजाय अपने toenails के लिए एक बॉलपेन हथौड़ा ले लेंगे। यह हर नेटवर्किंग क्लास में सामने पढ़ाया जाता है जो हम सभी को कॉलेज में लेना था, इसलिए हम सभी ने इसे एक हजार बार सुना है। उस ने कहा, हममें से जो थोड़ी देर के लिए इधर–उधर रहे हैं और एक प्रमाणीकरण Exam ली है या दो यह भी समझते हैं कि आमतौर पर कुछ आसान Exam उत्तर मिलते हैं–बशर्ते आप यह समझें कि वे क्या पूछ रहे हैं। मैं आपको एक ही सामान के साथ बोर नहीं करने जा रहा हूं जिसे आपने पहले सुना है या एक लाख बार पढ़ा है, जैसा कि पहले कहा गया था, आपको यह पहले से ही पता होना चाहिए। हालांकि, मैं क्या करने जा रहा हूं, ताकि आपके लिए एक त्वरित गति प्रदान की जा सके, आपको अपनी स्मृति को ताज़ा करने की आवश्यकता होगी।

मैंने अपनी समीक्षा के लिए इस विषय पर फिर से जाने के सवीत्तम तरीके के बारे में लंबा और कठिन सोचा, और तय किया कि मैं उसी पुराने बोरिंग तरीके से बात करूँगा। इसके बजाय, आइए एक नेटवर्क के निर्माण के लेंस के माध्यम से OSI संदर्भ मॉडल में दर्शाए गए दो कंप्यूटरों के बीच संचार सत्र के 10,000–फुट ओवरहेड दृश्य को देखें – विशेष रूप से यह पता लगाने की कोशिश करके कि आप जमीन से नेटवर्क का निर्माण कैसे करेंगे। शर्मन, श्री पीबॉडी और मेरे साथ वेकबैक मशीन में कदम, और नेटवर्किंग का आविष्कार होने से पहले हम वापस चले गए। आपको इसे कैसे करना होगा?

सबसे पहले, वहाँ बैठे उन दो कंप्यूटरों को देखकर आपस में बात करना चाहते हैं, आप अपनी आँखों के सामने जो सही है उसकी मूल बातों पर विचार कर सकते हैं: आप अपने कंप्यूटरों को एक साथ

जोड़ने के लिए क्या उपयोग करेंगे ताकि वे सिग्नल संचारित कर सकें? दूसरे शब्दों में, आप किस मीडिया का उपयोग करेंगे? कई विकल्प हैं: कॉपर केबलिंग, ग्लास ट्यूब, यहां तक कि रेडियो तरंगें, अन्य। और इस पर निर्भर करता है कि आप उनमें से किसे चुनते हैं, आपको यह पता लगाना होगा कि उपयोग करने योग्य जानकारी संचारित करने के लिए उनका उपयोग कैसे करें। आप दूसरे छोर पर कंप्यूटर से कुछ करने के लिए तार पर एक विद्युत संकेत कैसे प्राप्त करेंगे? रेडियो तरंग के किस भाग का उपयोग आप किसी शब्द या रंग को वर्तनी के लिए कर सकते हैं? इन सबसे ऊपर, आपको कनेक्टर्स, इंटरफेस और हस्तक्षेप के लिए कैसे खाते हैं, यह जानने की आवश्यकता होगी। और वह सिर्फ लेयर 1 (भौतिक परत) है, जहां सब कुछ बस बिट्स है – अर्थात, 1 और 0 का।

लेयर 2 तब आपके नेटवर्क को बढ़ाने में शामिल सवालों के जवाब देने में मदद करता है। यह पता लगाने में कि आप इस पूरी चीज़ का निर्माण कैसे करेंगे, यदि आप दो से अधिक नोड्स को जुड़ने की अनुमति देने का निर्णय लेते हैं, तो आप एड्रेसिंग को कैसे संभालेंगे? केवल दो प्रणालियों के साथ, यह कोई चिंता की बात नहीं है – भेजे गए सब कुछ दूसरे छोर पर आदमी द्वारा प्राप्त किया जाता है – लेकिन यदि आप मिश्रण में तीन या अधिक जोड़ते हैं, तो आपको यह पता लगाना होगा कि संदेश को एक अद्वितीय पते के साथ कैसे भेजा जाए । और अगर आपके मीडिया को साझा किया जाता है, तो आप कैसे गारंटी देंगे कि हर किसी को बात करने का मौका मिलता है, और किसी का संदेश किसी और के लिए उछलता नहीं है? डेटा लिंक परत (परत)2) इसे फ्रेम का उपयोग करके संभालता है, जो उच्च परतों से नीचे दिए गए सभी डेटा को एनक्रिप्ट करता है। फ्रेम्स ऐसे पते रखते हैं जो किसी विशेष नेटवर्क के अंदर एक मशीन की पहचान करते हैं।

और यदि आप अपने नेटवर्क से संदेश भेजना चाहते हैं तो क्या होगा? यह संबोधित करने के लिए स्थापित करने के लिए एक बात है ताकि प्रत्येक कंप्यूटर को पता हो कि पड़ोस के सभी अन्य कंप्यूटर कहाँ रहते हैं, लेकिन जितनी जल्दी या बाद में आप किसी अन्य पड़ोस को संदेश भेजना चाहते हैं – शायद एक और शहर भी। और आप निश्चित रूप से पूरी दुनिया के प्रत्येक कंप्यूटर का पता जानने के लिए प्रत्येक कंप्यूटर से अपेक्षा नहीं कर सकते। यह वह जगह है जहाँ लेयर 3 में पैकेट के साथ नेटवर्क एड्रेस और राउटिंग जानकारी का उपयोग किया जाता है। यह एक लिफाफे पर बहुत सारे ज़िप कोड की तरह काम करता है। जबकि सड़क का पता (लेयर से भौतिक पता)2) का उपयोग भौतिक नेटवर्क के अंदर प्राप्तकर्ता को परिभाषित करने के लिए किया जाता है, लेयर 3 से नेटवर्क एड्रेस उस मार्ग के साथ राउटर को बताता है जो संदेश के लिए पड़ोस (नेटवर्क) है।

अन्य विचार तब विश्वसनीय वितरण और प्रवाह नियंत्रण जैसे खेल में आते हैं। यदि आप इसे प्राप्त करने वाले को कोई विचार नहीं दे रहे हैं, तो आप निश्चित रूप से एक संदेश को नष्ट नहीं करना चाहेंगे; फिर से, आप संदेश के बारे में क्या चाहते हैं, इस पर निर्भर करता है। और आप निश्चित रूप से आपके द्वारा भेजे गए संदेशों को संभालने के लिए मीडिया की क्षमता को अभिभूत नहीं करना चाहते हैं, इसलिए हो सकता है कि आप संदेश के विशाल बोल्डर को एक बार में हमारे मीडिया पर डालना न चाहें, जब इसे छोटे, अधिक प्रबंधनीय टुकड़ों में काट दिया जाए। अधिक मायने रखता है। अगली परत, Transport, आपके लिए और इसे संभालती है। लेयर 4 में, खंड संदेश के विश्वसनीय अंत–टू–एंड वितरण के साथ–साथ त्रुटि सुधार (लापता सेगमेंट के पुनर्प्राप्ति के माध्यम से) और प्रवाह नियंत्रण को संभालता है।

इस बिंदु पर आपने सफलता के लिए चरण निर्धारित किया है। एक सिग्नल ले जाने के लिए मीडिया है (और आपने यह पता लगाया है कि उस मीडिया पर उस सिग्नल को कैसे एनकोड करना है), अपने नेटवर्क के अंदर और बाहर को संबोधित किया जाता है, और आपने फ्लो कंट्रोल और विश्वसनीयता जैसी चीजों का ध्यान रखा है। अब खुद मशीनों की ओर ऊपर की ओर देखने का समय है और सुनिश्चित करें कि उन्हें पता है कि उन्हें कैसे करना है। अगली तीन परतें (नीचे से ऊपर तक– सत्र, प्रस्तुति और अनुप्रयोग) डेटा को स्वयं संभालती हैं। सत्र परत एक सैद्धांतिक इकाई के रूप में अधिक है, जिसमें डेटा का कोई वास्तविक हेरफेर नहीं है – इसका काम सत्र को खोलना, बनाए रखना और बंद करना है। प्रेजेंटेशन लेयर को एक संदेश को एक प्रारूप में रखने के लिए डिज़ाइन किया गया है जिसे सभी सिस्टम समझ सकते हैं। उदाहरण के लिए, माइक्रोसॉफ्ट आउटलुक में गढ़ा गया एक ई–मेल आवश्यक रूप से आउटलुक चलाने वाली मशीन द्वारा प्राप्त नहीं किया जा सकता है, इसलिए इसे किसी ऐसे रिसीवर में अनुवाद किया जाना चाहिए जो किसी भी नेटवर्क पर डिलीवरी के लिए शुद्ध एएससीआईआई कोड की तरह समझ सकता है। अनुप्रयोग परत में सभी प्रोटोकॉल होते हैं जो उपयोगकर्ता को नेटवर्क पर और उसके आसपास जानकारी तक पहुंचने की अनुमति देते हैं। उदाहरण के लिए, एफ़टीपी उपयोगकर्ताओं को नेटवर्क में फ़ाइलों को Transport करने की अनुमति देता है, एसएमटीपी ई–मेल ट्रैफ़िक के लिए प्रदान करता है, और एचटीटीपी आपको काम के दौरान इंटरनेट पर सर्फ करने की अनुमति देता है जबकि आप कुछ और कर रहे हैं। ये तीन परतें स्टैक के "डेटा लेयर" को बनाती हैं, और वे सीधे टीसीपी / आईपी स्टैक के एप्लीकेशन लेयर पर मैप करती हैं। इन तीन परतों में, प्रोटोकॉल डेटा यूनिट (PDU) को डेटा कहा जाता है। परतें, और प्रोटोकॉल के उदाहरण जो आपको उनमें मिलेंगे, चित्र 1.1 में दिखाए गए हैं।

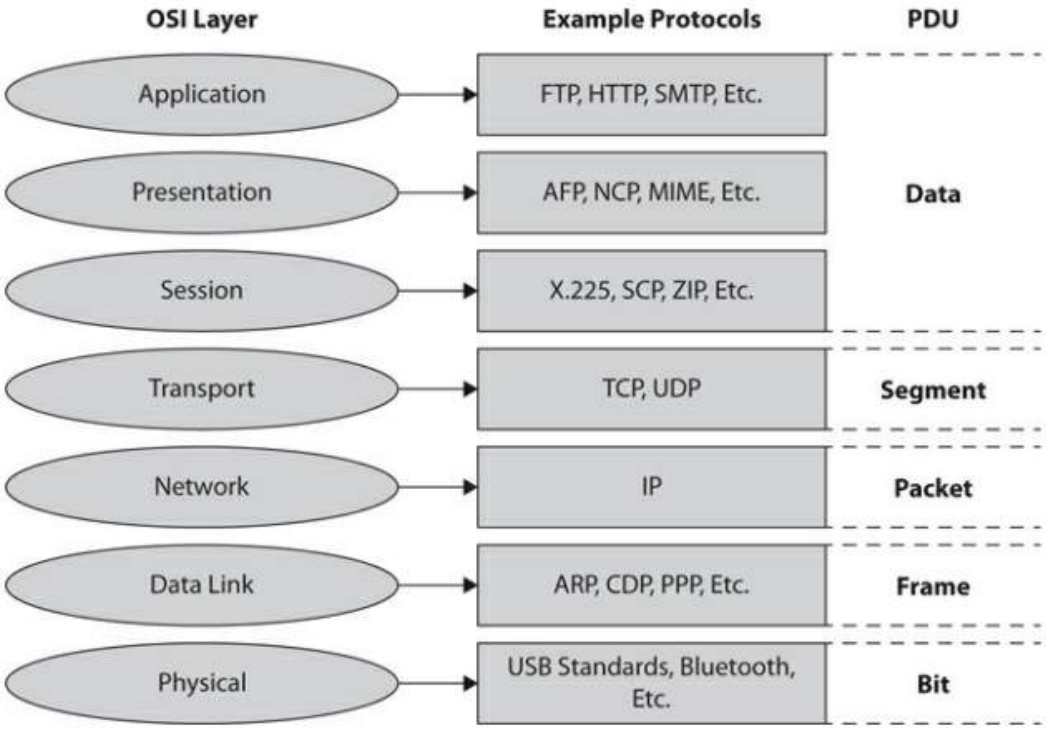


Figure 1-1 OSI reference model

Exam पर अपने OSI ज्ञान का परीक्षण करें कि प्रोटोकॉल डेटा यूनिट किस लेयर के साथ जाती है, इस सवाल के रूप में कुछ सरल नहीं होगा। बल्कि, आपसे ऐसे प्रश्न पूछे जाएंगे जो मॉडल के ज्ञान में मदद करेंगे; यह जानना कि किसी दिए गए स्तर पर क्या होता है, यह याद रखने में मदद करेगा कि प्रश्न किस टूल या प्रोटोकॉल के बारे में पूछ रहा है। एनाग्रम आपकी याददाश्त में मदद कर सकता है: "ऑल पीपल सीम टू नीड डेली प्लानिंग" परतों को सीधा रखेगा, और "डू सार्जेंट पे फॉर बीयर" परतों के साथ पीपीयू से मेल खाएगा।

TCP/IP Overview

यह ध्यान में रखते हुए कि आप यह पहले से ही जानने वाले हैं, हम इस विषय पर अधिक समय नहीं दे रहे हैं। उस ने कहा, यह आपकी सफलता के लिए महत्वपूर्ण है कि टीसीपी / आईपी नेटवर्किंग की

मूल बातें आपके जीवन के अन्य महत्वपूर्ण पहलुओं की तरह आपके न्यूरॉन्स में भी सीमित हैं, जैसे कि मॉम का जन्मदिन, लालफीताशाही पर आकार और बैग की सीमा, बोबीन का उचित अनुपात कुछ भी आप इसे मिलाते हैं, और रोलर पर टॉयलेट पेपर रखने का उचित तरीका (पेपर को नीचे खींचो, कभी ऊपर नहीं)। यह एक त्वरित पूर्वावलोकन होगा, और हम बाद के अध्यायों में इसे फिर से दोहराएंगे (और दोहराएंगे)।

टीसीपी / आईपी संचार प्रोटोकॉल का एक सेट है जो एक नेटवर्क पर मेजबान को एक दूसरे से बात करने की अनुमति देता है। प्रोटोकॉल के इस सूट को एक स्तरित स्टैक में व्यवस्थित किया गया है, जो कि OSI संदर्भ मॉडल की तरह है, जिसमें प्रत्येक परत एक विशिष्ट कार्य करती है। चित्र 1–2 में टीसीपी / आईपी स्टैक दिखाया गया है।

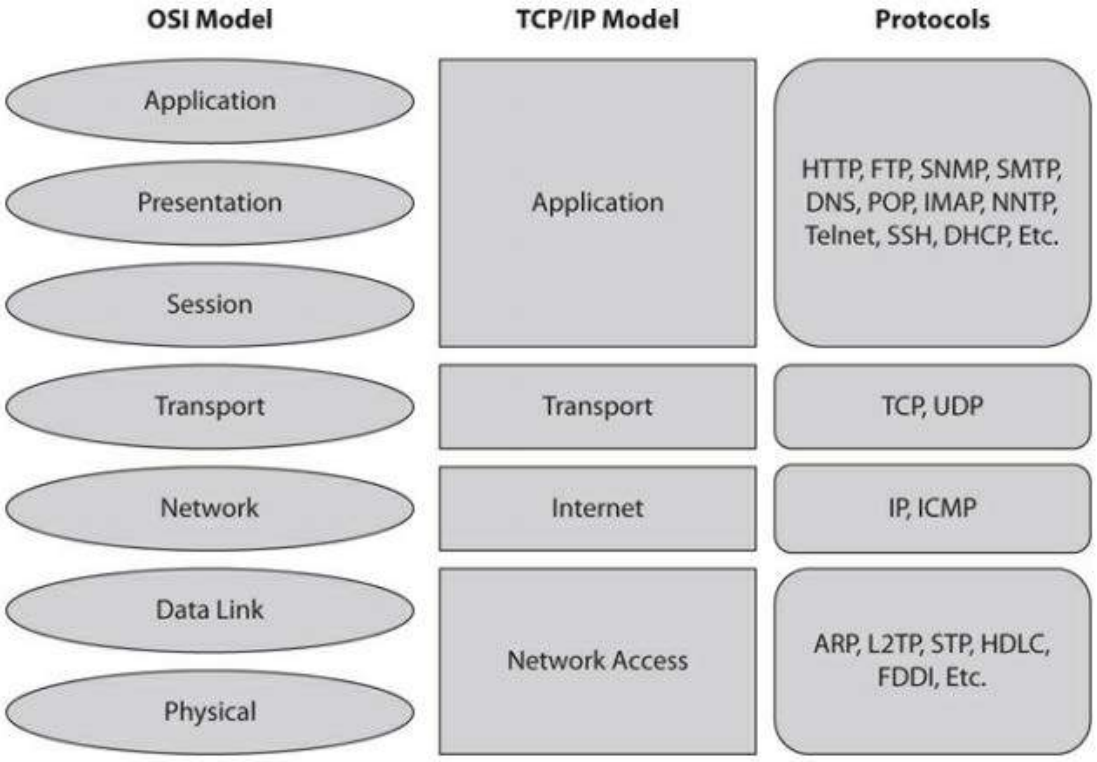


Figure 1-2 TCP/IP stack

इस अध्याय को शुरू करने के तरीके के अनुसार, चलो एक ही सामान से बचें जो आपने शायद एक हजार बार पहले ही सुना हो और बस एक मशीन से दूसरी मशीन के लिए एक संदेश का पालन करें टीसीपी /आईपी नेटवर्क। इस तरह, मुझे उम्मीद है कि सभी मूल बातें जो आपको बिना आँसू और उबाऊ की आवश्यकता के बिना टकराएंगी

आप इस अध्याय के बाकी हिस्सों को पूरी तरह से छोड़ दें। ध्यान रखें कि किसी भी सत्र में एक साथ कई गोइंग–ऑन हैं, इसलिए मैं चीजों को गति देने के लिए कुछ स्वतंत्रता ले सकता हूं।

मान लीजिए, उदाहरण के लिए, उपयोगकर्ता जो सीजन के सलामी बल्लेबाज के लिए तैयार होना चाहता है और अपने पसंदीदा विश्वविद्यालय अलबामा फुटबॉल गियर के लिए थोड़ी ऑनलाइन खरीदारी करने का फैसला करता है। जो अपने ब्राउज़र को खोलकर और अपनी पसंदीदा वेबसाइट के लिए अनुरोध करके टाइप करना शुरू करता है। उनके कंप्यूटर में अब ब्राउज़र से एक डेटा अनुरोध है जिसे वह देखता है और निर्धारित करता है कि आंतरिक रूप से उत्तर नहीं दिया जा सकता है। क्यूं कर? क्योंकि ब्राउज़र एक ऐसा पेज चाहता है जो स्थानीय स्तर पर संग्रहित न हो। इसलिए, अब अनुरोध का जवाब देने के लिए एक नेटवर्क इकाई की खोज की जा रही है, यह उस प्रोटोकॉल को चुनता है जो जानता है कि इस अनुरोध का उत्तर वापस आ जाएगा (इस मामले में, HTTP के लिए पोर्ट 80) और एक साथ रखना शुरू करता है जो एक सत्र बन जाएगा – एक गुच्छा किसी लक्ष्य को पूरा करने के लिए आगे और पीछे भेजे जाने वाले सेगमेंट।

चूंकि यह एक ईथरनेट टीसीपी / आईपी नेटवर्क है, जो के कंप्यूटर विशिष्ट क्रम में व्यवस्थित बिट्स के प्रारूप का उपयोग करके अन्य

प्रणालियों से बात करते हैं। एक विशिष्ट क्रम में बिट्स के इन संग्रहों को फ्रेम कहा जाता है (चित्र 1–3 एक मूल ईथरनेट फ्रेम दिखाता है), अंदर से बाहर से निर्मित होते हैं, और ऊपरी परतों से दी गई जानकारी पर भरोसा करते हैं। इस उदाहरण में, एप्लिकेशन लेयर एक HTTP रिक्वेस्ट (डेटा) को ट्रांसपोर्ट लेयर पर "हैंड डाउन" करेगी। इस परत पर, जो का कंप्यूटर HTTP अनुरोध को देखता है और (क्योंकि यह जानता है कि HTTP आमतौर पर इस तरह से काम करता है) जानता है कि यह कनेक्शन–उन्मुख सत्र होना चाहिए, जो कुछ भी खोए बिना जो कुछ भी मांगता है उसे सुनिश्चित करने के लिए तारकीय विश्वसनीयता सुनिश्चित करता है। यह उसके लिए ट्रांसमिशन कंट्रोल प्रोटोकॉल (टीसीपी) पर कॉल करता है। टीसीपी अंत स्टेशन के साथ संचार सत्र स्थापित करने के लिए संदेशों की एक श्रृंखला में बाहर निकल जाएगी, जिसमें चीजों को प्राप्त करने के लिए तीन–चरण हैंडशेक शामिल है। इस हैंडशेक में एक सिंक्रोनाइज़्ड सेगमेंट (SYN), एक सिंक्रोनाइज़्ड एविलेडिंग सेगमेंट (SYN / ACK) और एक Acknowledgment सेगमेंट (ACK) शामिल हैं। इनमें से पहला– SYN खंड दूसरे कंप्यूटर से पूछ रहा है कि क्या यह जाग रहा है और बात करना चाहता है – इंटरनेट परत को संबोधित करने के लिए नीचे सौंप दिया गया है।

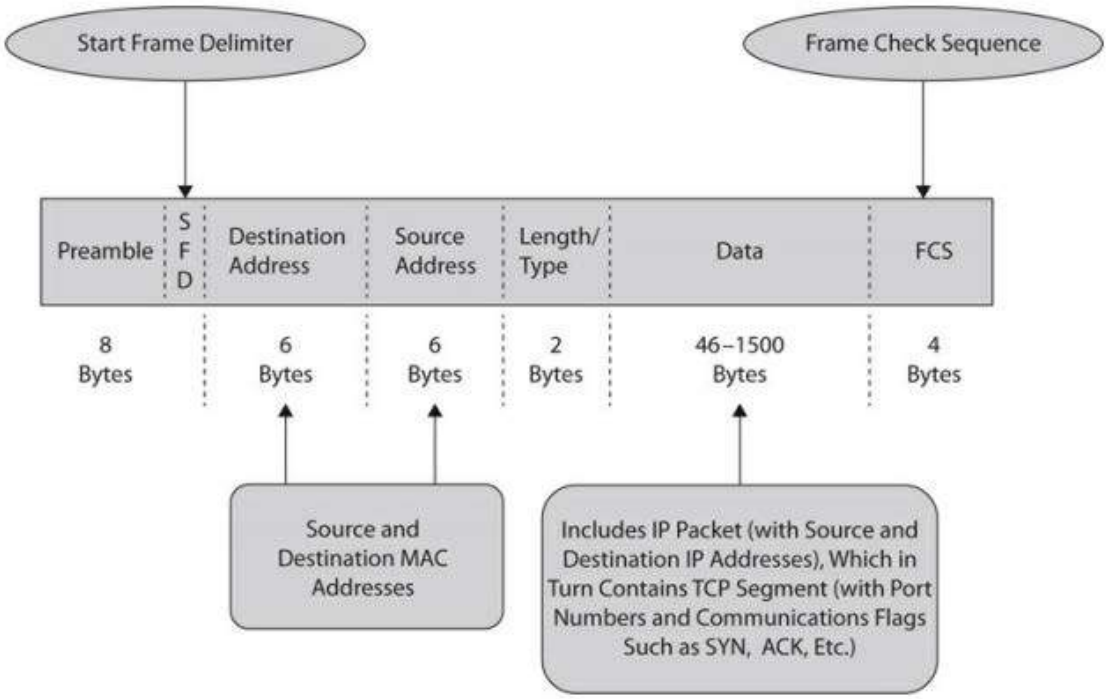


Figure 1-3 An Ethernet frame

51 इस प्रयास सप्ताह के अंत में, बॉब ने अपनी पीठ के पोर्च पर एक मेकर्स मार्क और एक आर्टुरो फ़ेंटे के साथ आराम किया, जो उसने किए गए सभी अच्छे सुरक्षा कार्यों को मुस्कुराते हुए और पुरस्कार के रूप में प्रदान किए गए उनके नेतृत्व का आनंद ले रहे थे। जोए ने अपने अपार्टमेंट में यह कहते हुए गुस्सा किया कि अब उनका काम तेजी से कठिन होगा। लेकिन जब बॉब शाम को अपने लॉरेल्स पर आराम करने के लिए ले गया, जोई ओपी के बचाव में काम करने, खरोंचने और खुदाई करने के लिए वापस चला गया। "एक दिन मुझे एक रास्ता मिल जाएगा। बस इंतजार करो और देखो। मैं नहीं रोकूंगा। कभी।"

अब, यह सिर्फ परिभाषाएँ पढ़ने से बेहतर नहीं था? यकीन है कि वहाँ कुछ छलांग थे, और बॉब निश्चित रूप से आदमी नहीं होगा ALE माप कर रहा है, लेकिन यह सब समझाने की कोशिश करने से

बेहतर है अन्यथा। इस खंड में प्रत्येक इटैलिकाइज्ड शब्द संभवतः आपकी Exam में दिखाई दे सकता है, और अब आप बस इस छोटी सी कहानी को याद रख सकते हैं और आप लगभग किसी भी चीज के लिए तैयार होंगे। लेकिन हालांकि यह मजेदार था, और मैंने इसे इस पुस्तक के शेष भाग में जारी रखने पर विचार किया (कथा इतनी अधिक मनोरंजक है), इसमें से कुछ एक गुजर इटैलिक संदर्भ की तुलना में थोड़ा अधिक है, इसलिए हम यहां तोड़ देंगे और वापस जाएंगे अधिक "अपेक्षित" लेखन।

CIA

किसी भी सुरक्षा मूलक चर्चा में एक और आधार आईटी सुरक्षा की पवित्र त्रिमूर्ति है: गोपनीयता, अखंडता और उपलब्धता (सीआईए)। चाहे आप एक नैतिक हैकर हों या नहीं, ये तीनों वस्तुएं सुरक्षा की पहचान हैं, जिनके लिए हम सभी प्रयास करते हैं। एक नैतिक हैकर के रूप में और साथ ही Exam में सफलता प्राप्त करने के लिए आपको प्रत्येक शब्द के दो पहलुओं से परिचित होना होगा: इस शब्द का अर्थ क्या है और इसके साथ कौन से हमले सबसे अधिक जुड़े हैं।

गोपनीयता, जानकारी की गोपनीयता और गोपनीयता को संबोधित करते हुए, अनधिकृत व्यक्तियों या प्रणालियों के लिए सूचना या डेटा के प्रकटीकरण को रोकने के लिए किए गए उपायों को संदर्भित करता है और इसे प्राप्त करने के लिए अधिकृत लोगों को जानकारी के उचित प्रकटीकरण को सुनिश्चित करता है। व्यक्ति के लिए गोपनीयता एक जरूरी है, इसके नुकसान को देखते हुए पहचान की चोरी, धोखाधड़ी और धन की हानि हो सकती है। एक व्यवसाय या सरकारी एजेंसी के लिए, यह और भी बुरा हो सकता है। प्रमाणीकरण के कुछ रूपों के भीतर पासवर्ड का उपयोग गोपनीयता सुनिश्चित करने के लिए अब तक का सबसे आम उपाय है, और पासवर्ड के खिलाफ हमले, आश्चर्यजनक रूप से पर्याप्त हैं, सबसे आम

गोपनीयता हमले हैं।

उदाहरण के लिए, किसी नेटवर्क में आपके लॉगऑन में आमतौर पर एक उपयोगकर्ता आईडी और एक पासवर्ड होता है, जो केवल यह सुनिश्चित करने के लिए डिज़ाइन किया गया है कि आपके पास उस विशेष उपकरण या नेटवर्क संसाधनों का सेट है। यदि कोई अन्य व्यक्ति आपकी उपयोगकर्ता आईडी और पासवर्ड प्राप्त करता है, तो उनके पास संसाधनों तक अनधिकृत पहुंच होगी और

“सुरक्षा के चार तत्व।” यह प्रमाणीकरण क्षेत्र के बाहर बहुत अधिक उपयोग नहीं किया जाता है, हालांकि इस शब्द का उपयोग अक्सर सबसे अधिक "वास्तविक" के रूप में किया जाता है।उदाहरण के लिए, डिजिटल हस्ताक्षर का उपयोग संदेश भेजने वाले व्यक्ति की प्रामाणिकता की गारंटी के लिए किया जा सकता है। परीक्षण के समय आओ, इससे मदद मिल सकती है।

Access Control System

जब हम कंप्यूटर सुरक्षा के विषय पर होते हैं, तो मुझे लगता है कि यह कदम पीछे खींचने में मददगार हो सकता है और हम सभी को यहां कैसे मिला, और इसके कुछ मानकों और कुछ शब्दों के माध्यम से संक्षिप्त जानकारी दें। कंप्यूटिंग और नेटवर्किंग के शुरुआती दिनों में, यह कहना बहुत सुरक्षित है कि किसी की टू–डू सूची में सुरक्षा अधिक नहीं थी। तथ्य की बात के रूप में, अधिकांश उदाहरणों में सुरक्षा पर भी विचार नहीं किया गया था, और दुर्भाग्य से यह तब तक नहीं था जब तक कि चीजें हाथ से बाहर नहीं निकलने लगीं कि किसी ने वास्तव में इसमें कोई प्रयास करना शुरू नहीं किया। बहुत सारी सुरक्षा के बारे में दुखद सच्चाई यह है कि यह एक प्रतिक्रियावादी रुख से बाहर आया, और बहुत कम सोचा गया कि इसे एक सक्रिय प्रयास के रूप में रखा गया– अपेक्षाकृत हाल ही में,

वैसे भी।

यह कहना नहीं है कि किसी ने भी कोशिश नहीं की। तथ्य की बात है, 1983 में अमेरिकी रक्षा विभाग के कुछ स्मार्ट लोगों ने सूचना के संरक्षण (सरकार की जानकारी, जो है) की भविष्य की आवश्यकता को देखा और राष्ट्रीय कंप्यूटर सुरक्षा केंद्र (NCSC) बनाने के लिए NSA के साथ काम किया। इस समूह को एक साथ मिला और सभी प्रकार के सुरक्षा मैनुअल और चरणों का निर्माण किया, और उन्हें "रेनबो सीरीज़" नामक पुस्तक श्रृंखला में प्रकाशित किया। इस प्रयास का केंद्र बिंदु "ऑरेंज बू" के रूप में सामने आया, जिसे ट्रस्टेड कंप्यूटर सिस्टम इवैल्यूएशन मानदंड (TCSEC) के रूप में जाना जाता है।

TCSEC एक संयुक्त राज्य सरकार का रक्षा विभाग (DoD) मानक था, जिसका लक्ष्य कंप्यूटर सिस्टम में निर्मित कंप्यूटर सुरक्षा नियंत्रणों की प्रभावशीलता के परीक्षण के लिए बुनियादी आवश्यकताओं को निर्धारित करना था। यह विचार सरल था: यदि आपका कंप्यूटर सिस्टम (नेटवर्क) वर्गीकृत जानकारी को संभालने जा रहा है, तो उसे बुनियादी सुरक्षा सेटिंग्स का पालन करने की आवश्यकता है। TCSEC ने परिभाषित किया कि कैसे इन नियंत्रणों का मूल्यांकन किया जाए और उन्होंने कितना अच्छा काम किया। ऑरेंज बुक (अपने समय के लिए) की सेटिंग्स, मूल्यांकन और नोटिस को अच्छी तरह से सोचा गया और समय की कसौटी पर अपनी योग्यता साबित की, सभी तरह से जीवित रहे 2005. हालाँकि, जैसा कि सुरक्षा में कोई भी आपको बता सकता है, कुछ भी हमेशा के लिए नहीं रहता है।

TCSEC ने अंततः सूचना प्रौद्योगिकी सुरक्षा मूल्यांकन (जिसे सामान्य मानदंड या CC के रूप में भी जाना जाता है) के लिए सामान्य

मानदंड के लिए रास्ता दिया।

आम मानदंड वास्तव में 1999 के बाद से आस–पास था, और अंत में पूर्वता ले ली2005. इसने विक्रेताओं को नियंत्रण और परीक्षण विधियों के एक निर्धारित मानक का पालन करके अपनी जगह की सुरक्षा के बारे में दावे करने का एक तरीका प्रदान किया, जिसके परिणामस्वरूप कुछ मूल्यांकन मूल्यांकन स्तर (EAL) कहा जाता है। उदाहरण के लिए, एक विक्रेता एक उपकरण, एप्लिकेशन या कंप्यूटर सिस्टम बना सकता है और सुरक्षा घोषणा करने की इच्छा कर सकता है। वे तब EAL (स्तर 1) पर अपने सिस्टम का परीक्षण करने के लिए नियंत्रण और परीक्षण प्रक्रियाओं का पालन करेंगे।) वे चाहते थे। परीक्षण सफल होने पर, विक्रेता दावा कर सकता है "सफलतापूर्वक EAL–4 पर परीक्षण किया गया।"

आम मानदंड, मूल रूप से, एक परीक्षण मानक है जो किसी उत्पाद से कमजोरियों को कम करने या हटाने से पहले डिज़ाइन किया गया है। EAL के अलावा, तीन अन्य शब्द इस प्रयास से जुड़े हैं जिन्हें आपको याद रखना होगा:

- **Target of evaluation (TOE) -** क्या परीक्षण किया जा रहा है।
- **Security target (ST) -** टीओई और सुरक्षा आवश्यकताओं का वर्णन करने वाला दस्तावेज।

- **Protection profile (PP) -** विशेष रूप से परीक्षण किए जा रहे उत्पाद के type के लिए सुरक्षा आवश्यकताओं का एक समूह।

जबकि इसके लिए पूरी तरह से अधिक है, यह कहना पर्याप्त है कि सीसी को एक आश्वासन प्रदान करने के लिए डिज़ाइन किया गया था कि सिस्टम एक विशिष्ट सुरक्षा स्तर के अनुसार डिज़ाइन, कार्यान्वित और परीक्षण किया गया है। इसका उपयोग सरकारी प्रमाणपत्रों के आधार के रूप में किया जाता है और आमतौर पर अमेरिकी सरकारी एजेंसियों के लिए इसका परीक्षण किया जाता है।

अंत में सुरक्षा और परीक्षण के संबंध में शब्दावली और इतिहास के माध्यम से हमारे जॉट में, हमारे पास निपटने के लिए कुछ शब्द हैं। इनमें से एक अभिगम नियंत्रण की समग्र अवधारणा है। मूल रूप से अभिगम नियंत्रण का अर्थ है कुछ चयनात्मक तरीके से संसाधन तक पहुँच को रोकना। आपके द्वारा ध्वनि को वास्तव में बुद्धिमान (विषय, सर्जक, प्राधिकरण, और इसी तरह) बनाने के लिए इस पर चर्चा करने के बारे में सभी type की शर्तें हैं, लेकिन मैं शब्दावली के लिए वह सब छोड़ दूँगा। यहां, हम एक्सेस कंट्रोल लागू करने के कुछ तरीकों के बारे में बात करेंगे: अनिवार्य और विवेकाधीन।

अनिवार्य अभिगम नियंत्रण **(Mandatory access control)** (मैक के लिए संक्षिप्त) अभिगम नियंत्रण का एक तरीका है जहां सुरक्षा नीति को एक सुरक्षा व्यवस्थापक द्वारा नियंत्रित किया जाता है: उपयोगकर्ता स्वयं पहुँच नियंत्रण सेट नहीं कर सकते हैं। मैक में, ऑपरेटिंग सिस्टम एक संसाधन तक पहुंचने के लिए एक इकाई की क्षमता को सीमित करता है (या सिस्टम के भीतर किसी type का कार्य करने के लिए)। उदाहरण के लिए, एक इकाई (जैसे कि एक प्रक्रिया) एक वस्तु (जैसे कि फाइलें, टीसीपी या यूडीपी पोर्ट, और इसी तरह) तक पहुंचने या बदलने का प्रयास कर सकती है।

संसाधन, उपयोगकर्ता अधिकारों को परिभाषित करना, संवेदनशील जानकारी के प्रकटीकरण को रोकना, और उपयोगकर्ताओं और

भागीदारों के लिए कानूनी दायित्व को संबोधित करना। विभिन्न सुरक्षा नीति type की दुनिया हैं, जिनमें से कुछ सामान्य लोगों की पहचान की गई है:

- **Access Control Policy -** यह उन संसाधनों की पहचान करती है जिन्हें उन संसाधनों तक पहुंच को नियंत्रित करने के लिए सुरक्षा और नियमों की आवश्यकता होती है।

- **Information Security Policy -** यह कर्मचारियों को पहचानती है कि किस कंपनी के सिस्टम का उपयोग किया जा सकता है, उनका क्या उपयोग नहीं किया जा सकता है और नियमों को तोड़ने के लिए क्या परिणाम हैं। आमतौर पर कर्मचारियों को संसाधनों तक पहुंचने से पहले एक प्रति पर हस्ताक्षर करने की आवश्यकता होती है। इस नीति के Version को स्वीकार्य उपयोग नीति के रूप में भी जाना जाता है।

- **Information Protection Policy -** यह सूचना संवेदनशीलता स्तरों को परिभाषित करती है और उन स्तरों तक पहुंच रखती है। यह यह भी बताता है कि डेटा कैसे संग्रहीत, संचरित और नष्ट हो जाता है।

- **Password Policy -** यह संगठन के भीतर लंबाई, जटिलता, अधिकतम और न्यूनतम आयु और पुन: उपयोग सहित पासवर्ड के बारे में कल्पना करने योग्य सब कुछ को परिभाषित करता है।

- **E-mail Policy -** को कभी–कभी ई–मेल सुरक्षा नीति भी कहा जाता है, यह कंपनी ई–मेल प्रणाली के उचित उपयोग को

संबोधित करती है।

- **Information Audit Policy-** यह संगठन के भीतर सुरक्षा ऑडिट करने के लिए रूपरेखा को परिभाषित करता है। कब, कहां, कैसे, कितनी बार, और कभी–कभी यहां तक कि जो सूचना सुरक्षा ऑडिट करता है, उसका वर्णन यहां किया गया है।

कई अन्य type की सुरक्षा नीतियां हैं, और हम आगे बढ़ सकते हैं, लेकिन आपको यह विचार मिलता है। अधिकांश नीतियों को केवल नाम के आधार पर समझना काफी आसान है। उदाहरण के लिए, यह निर्धारित करना कठिन नहीं होना चाहिए कि रिमोट एक्सेस पॉलिसी यह पहचानती है कि सिस्टम के लिए दूरस्थ पहुंच कौन हो सकती है और वे उस एक्सेस को कैसे प्राप्त कर सकते हैं। अन्य आसान पहचान नीतियों में उपयोगकर्ता खाता, फ़ायरवॉल प्रबंधन, नेटवर्क कनेक्शन और विशेष पहुंच शामिल हैं।

अंत में, और मैं इसमें शामिल हो गया क्योंकि मैं आप लोगों को असली दुनिया में पहले से ही गुनगुनाते हुए सुन सकता हूं, लेकिन यह विश्वास है या नहीं, ईसी–काउंसिल नीति के माध्यम से यह भी देखता है कि उपयोगकर्ताओं पर यह कितना कठिन है। एक उचित नीति मूल रूप से व्यापक है, जबकि एक अनुमेय नीति केवल उन चीजों को अवरुद्ध करती है जो हैं।

EXAM TIP - इस चर्चा में कमिटमेंट के चार अन्य शब्द हैं स्मृति के लिए। मानक अनिवार्य नियम हैं जिनका उपयोग स्थिरता प्राप्त करने के लिए किया जाता है। आधारभूत आवश्यक न्यूनतम सुरक्षा स्तर प्रदान करते हैं। दिशानिर्देश हैं उपयोगकर्ताओं के लिए लचीली

अनुशंसित कार्रवाइयाँ हैं जो कि नहीं है पालन करने के लिए मानक। और अंत में, प्रक्रियाएं चरण–दर–चरण विस्तृत हैं किसी कार्य या लक्ष्य को पूरा करने के निर्देश।

Introduction to Ethical Hacking

अधिकांश लोगों को हैकर शब्द को परिभाषित करने के लिए कहें, और वे तुरंत एक तस्वीर देंगे अंधेरा कमरा, कई मॉनिटर हरे भरे पाठ को स्क्रॉल करते हुए घिसते हैं स्क्रीन, और कोने में एक छायादार चरित्र गुस्से में टाइपिंग ए पर किसी चीज को तोड़ने या चुराने के प्रयास में कीबोर्ड। दुर्भाग्य से, यह बहुत कुछ सच है, और दुनिया भर में बहुत सारे लोग इन गतिविधियों में सक्रिय रूप से भाग लेते हैं उसी उद्देश्य के लिए। हालांकि, यह महसूस करना महत्वपूर्ण है कि मतभेद हैं इस दायरे में अच्छे लोगों और बुरे लोगों के बीच। यह इसका लक्ष्य है अनुभाग आपके लिए दो समूहों को परिभाषित करने में मदद करने के लिए, साथ ही साथ कुछ पृष्ठभूमि प्रदान करता है। चाहे महान या बुरे उद्देश्यों के लिए, हैकिंग की कला एक ही है। उपकरण, तकनीक, ज्ञान और कौशल को बायपास करने के लिए एक विशेष सेट का उपयोग करना कंप्यूटर सुरक्षा उपाय किसी को कंप्यूटर में "हैक" करने की अनुमति देता है या नेटवर्क। इन उपकरणों और तकनीकों के उनके उपयोग के पीछे का उद्देश्य वास्तव में है सवाल में ही बात है। जबकि कुछ इन उपकरणों और तकनीकों का उपयोग करते हैं व्यक्तिगत लाभ या लाभ, अच्छे लोग बेहतर बचाव के लिए उनका अभ्यास करते हैं उनके सिस्टम और, इस प्रक्रिया में, बुरे लोगों को पकड़ने के तरीके के बारे में जानकारी प्रदान करते हैं।

Hacking Terminology

किसी भी अन्य कैरियर क्षेत्र की तरह, हैकिंग (एथिकल हैकिंग) का अपना लिंगो और ए है जानने के लिए असंख्य। उदाहरण के लिए,

हैकर्स स्वयं, विभिन्न हैं शर्तों और वर्गीकरण में गिर करने के लिए। उदाहरण के लिए, आप पहले से ही जानते होंगे एक सक्रिप्ट किडी एक व्यक्ति है जो हैकिंग तकनीकों में अशिक्षित है जो बस स्वतंत्र रूप से उपलब्ध (लेकिन पुराने और पुराने) उपकरण का स्वतंत्र रूप से उपयोग करता है और इंटरनेट पर तकनीक। और आप शायद पहले से ही जानते हैं कि एक सनकी है
कोई है जो मुक्त करने के लिए दूरसंचार प्रणालियों में हेरफेर करता है
कहता है। लेकिन इस खंड से आप अपरिचित हैं के साथ मदद करने में सक्षम हो सकता है। शायद आपको बस परीक्षण के लिए एक संदर्भ बिंदु की आवश्यकता है अध्ययन, या शायद यह सब आपके लिए नया है; किसी भी तरह, शायद वहाँ एक होगा Exam में मदद करने के लिए यहाँ डला या दो।

अंतहीन परिभाषाओं और के लिए 100–पृष्ठ के अध्याय से बचने के प्रयास में इस Exam के लिए अध्ययन में अपनी पवित्रता बनाए रखने में आपकी सहायता करने का प्रयास, हम आपके द्वारा याद की जाने वाली अधिक प्रासंगिक जानकारी के साथ चिपके रहेंगे, और मैं आपको अधिक के लिए इस पुस्तक के अंत में शब्दावली का उपयोग करने की सलाह देता हूं
जानकारी। आप इन शब्दों को पूरी किताब में वैसे भी उपयोग करते देखेंगे, और उनमें से ज्यादातर अपने दम पर पता लगाने के लिए काफी आसान है, लेकिन छूट नहीं है परिभाषाएँ आपको शब्दावली में मिलेंगी। इसके अलावा, मैंने वास्तव में कड़ी मेहनत की शब्दावली – अगर यह किसी का ध्यान नहीं गया तो यह शर्म की बात होगी।

एक्जाम टीआईपी परिभाषा प्रश्न Exam में नो–ब्रेनर होना चाहिए। सीखना हैकर प्रकार, एक हैक के चरणों, और अध्याय में अन्य परिभाषाएँ– आसान याद नहीं है।

Hacker Classifications: The Hats

आप एक हैकर को अनगिनत तरीकों से वर्गीकृत कर सकते हैं, लेकिन "हैट" प्रणाली लगती है समय की कसौटी पर खरा उतरा। मुझे नहीं पता कि क्या है क्योंकि हैकर्स पसंद करते हैं पश्चिमी फिल्में या हम सब सिर्फ चरवाहे फैशन के साथ मोहित हैं, लेकिन यह है निश्चित रूप से आप अपनी Exam में बार–बार देखेंगे।

सामान्य रूप से हैकिंग समुदाय को तीन अलग–अलग में वर्गीकृत किया जा सकता है वर्गीकरण: अच्छा, बुरा और अनिर्दिष्ट। आईटी की दुनिया में सुरक्षा, इस पदनाम को टोपी के रंग के रूप में दिया गया है और इसके लिए काफी आसान होना चाहिए आप पर नज़र रखने के लिए

- सफेद टोपी अच्छे लोगों को ध्यान में रखते हुए, ये नैतिक हैकर हैं,परीक्षण और सुधार के विशिष्ट लक्ष्य के लिए एक ग्राहक द्वारा काम पर रखा गया सुरक्षा या अन्य रक्षात्मक उद्देश्यों के लिए। सफेद टोपियों का अच्छी तरह से सम्मान किया जाता है और बिना पूर्व सहमति के उनके ज्ञान और कौशल का उपयोग न करें। सफेद
  टोपी को सुरक्षा विश्लेषक के रूप में भी जाना जाता है।

- ब्लैक हैट्स ने बुरे लोगों को माना, ये अवैध रूप से पटाखे हैं व्यक्तिगत लाभ या दुर्भावनापूर्ण इरादे के लिए अपने कौशल का उपयोग करना। वे चाहते हैं चोरी करना (कॉपी करना) या डेटा को नष्ट करना और संसाधनों तक पहुँच को अस्वीकार करना और सिस्टम। काली टोपी अनुमति या सहमति के लिए नहीं पूछती है।

- ग्रे हैट को वर्गीकृत करने के लिए सबसे कठिन समूह, ये हैकर्स न तो हैं अच्छा और न ही बुरा। सामान्यतया, ग्रे टोपी के दो सबसेट होते हैं–जो केवल हैकिंग टूल और तकनीकों के बारे में उत्सुक हैं और जिन लोगों को ऐसा लगता है कि यह उनकी ड्यूटी है, ग्राहक की अनुमति के साथ या बिना, सिस्टम में सुरक्षा खामियों को प्रदर्शित करने के लिए। किसी भी मामले में, हैकिंग ग्राहक की स्पष्ट अनुमति और दिशा के बिना आमतौर पर एक अपराध है।

ध्यान दें कि बहुत से अर्थ हैकर प्रकार के रोजगार पाए गए हैं
एक सिस्टम में हैक करके और फिर पीड़ित को सूचित करके सुरक्षा क्षेत्र
सुरक्षा खामियां ताकि उन्हें ठीक किया जा सके। हालांकि, कई और अधिक पाया गया है एक ही बात का प्रयास जेल के लिए उनके रास्ते। चाहे आपके इरादे कुछ भी हों, बिना स्वीकृति के हैकिंग तकनीक का अभ्यास न करें। आप अपनी टोपी सोच सकते हैं ग्रे है, लेकिन मैं गारंटी देता हूं कि पीड़ित केवल काला देखता है।

जब हम इस विषय पर हैं, तो इस समुदाय का एक अन्य सबसेट इसका उपयोग करता है एक कारण या एक राजनीतिक एजेंडा को आगे बढ़ाने के लिए कौशल और प्रतिभा। ये लोग सर्वर हैक करना, वेबसाइटों को ख़राब करना, वायरस पैदा करना, और आम तौर पर सभी प्रकार की समस्याओं को मिटा देना साइबरस्पेस में इस धारणा के तहत कि उनके कार्य कुछ मजबूर करेंगे सामाजिक परिवर्तन या किसी ऐसी चीज़ पर प्रकाश डालना जो उन्हें एक राजनीतिक अन्याय लगता है। यह मानव प्रकृति में कुछ नई विसंगति नहीं है – लोग विरोध करते रहे हैं समय की सुबह के बाद से चीजें – यह सिर्फ

पिकेट के संकेतों से चली गई हैं और
बिट्स और बाइट्स के लिए मार्च। सामान्य तौर पर, इरादों की परवाह किए बिना, कार्य करता है हकीववाद आमतौर पर प्रकृति में अवैध हैं।

पागल पर हैकर सीमाओं का एक और वर्ग। कुछ हैकर्स तो संचालित होते हैं, इसलिए अपने काम को पूरा करने के इरादे से, वे इसे खींचने के लिए सब कुछ जोखिम में डालने को तैयार हैं बंद। जब तक हम नैतिक हैकर के रूप में, हम कुछ भी नहीं छू सकते हैं जब तक हम दिया जाता है
ऐसा करने के लिए सहमति व्यक्त करते हैं, ये हैकर बहुत से हक्टिविस्ट हैं और ऐसा महसूस करते हैं हैकिंग के लिए उनका कारण किसी भी संभावित सजा से अधिक है। को भी तैयार है उनकी गतिविधियों के लिए जोखिम समय जेल, तथाकथित आत्मघाती हैकर वास्तव में डरावना हैं
कोठरी में राक्षस। ये लोग झुलसी हुई पृथ्वी की मानसिकता में काम करते हैं और करते हैं अपनी खुद की सुरक्षा या स्वतंत्रता की परवाह नहीं, किसी और का जिक्र नहीं।

Exam TIP - ECC को भ्रमित करने के लिए मिश्रण में और अधिक परिभाषाएँ जोड़ना पसंद करता है मुद्दा। यहाँ कुछ अन्य याद रखने योग्य हैं: सक्रिप्ट किडी (अकुशल, उपयोग करना अन्य लिपियों और उपकरण), साइबर आतंकवाद (धार्मिक या राजनीतिक से प्रेरित) भय और बड़े पैमाने पर सिस्टम व्यवधान पैदा करने के लिए विश्वास), और राज्य द्वारा प्रायोजित हैकर (एक सरकार द्वारा नियोजित)।

Attack Types

इस परिचय के माध्यम से हमारी चहलकदमी में एक और क्षेत्र एक हैकर प्रयास कर सकता है विभिन्न प्रकार के हमलों की चिंता करता

है। इनमे से ज्यादातर पहचानना और प्रतीत करना काफी आसान है, कई बार, काफी मूर्खतापूर्ण तरीके से वर्गीकृत भी किया जाता है। आखिर, क्या आपको परवाह है कि अगर यह आपके लिए काम करता है तो हमले के प्रकार को क्या कहा जाता है? के लिये यह Exam, ईसी–काउंसिल इन सभी प्रकार के हमलों को मोटे तौर पर चार में परिभाषित करती है श्रेणियाँ।

- **Operating system (OS) attack** के हमले आम तौर पर बोलते हैं, इन हमलों सामान्य गलती को लक्षित करें जो कई लोग स्थापित करते समय करते हैं ऑपरेटिंग सिस्टम–सभी चूक को स्वीकार करना और छोड़ना। व्यवस्थापक बिना किसी पासवर्ड के खाता, सभी पोर्ट खुले छोड़ दिए गए, और अतिथि खाते (सूची हमेशा के लिए चल सकती है) सेटिंग्स के उदाहरण हैं इंस्टॉलर के बारे में भूल सकता है। इसके अतिरिक्त, ऑपरेटिंग सिस्टम हैं पूरी तरह से सुरक्षित कभी नहीं जारी किया – वे हो सकता है, अगर आप कभी जारी करने की योजना नहीं है उन्हें वास्तविक उपयोग के समय–सीमा के भीतर – तो एक पुराने के लिए क्षमता नव स्थापित ऑपरेटिंग सिस्टम में Vulnerability हमेशा के लिए एक प्लस है नैतिक हैकर।

- **Application-level attacks** ये वास्तविक पर हमले हैं प्रोग्रामिंग कोड और किसी एप्लिकेशन का सॉफ्टवेयर लॉजिक। हालांकि सबसे लोग अपने ओएस और नेटवर्क को हासिल करने के लिए जागरूक हैं, यह आश्चर्यजनक है कितनी बार वे अपने ओएस पर चल रहे एप्लिकेशन को छूट देते हैं और नेटवर्क। नेटवर्क पर कई एप्लिकेशन के लिए परीक्षण नहीं किया गया है उनकी रचना के हिस्से के रूप में कमजोरियां

और, जैसे, कई हैं उनमें निर्मित कमजोरियाँ। एक नेटवर्क पर अनुप्रयोग एक सोना है अधिकांश हैकर्स के लिए मेरा।

- **Shrink-wrap code attacks** ये अटैक बिल्टिन कोड का फायदा उठाते हैं और सक्रिप्ट ऑफ–द–शेल्फ अनुप्रयोगों के साथ आती हैं। "अक्सर इस हमले का वर्णन करने के लिए उपयोग किया जाता है प्रकार। जब आप कर सकते हैं तो कुछ पर हमला करने के लिए कोड लिखने में समय क्यों खर्च करें इसे पहले ही खरीद लें "shrink–wrapped"? ये सक्रिप्ट और कोड टुकड़े हैं स्थापना और प्रशासन को आसान बनाने के लिए डिज़ाइन किया गया है, लेकिन आगे बढ़ सकता है कमजोरियों अगर उचित रूप से प्रबंधित नहीं किया गया।

- **Misconfiguration attacks** ये हमले सिस्टम का फायदा उठाते हैं उद्देश्य या दुर्घटना से, उचित रूप से कॉनफ़िगर नहीं किए गए हैं सुरक्षा। पहले त्रिकोण और अधिकतम याद रखें "सुरक्षा के रूप में वृद्धि, उपयोग में आसानी और कार्यक्षमता घट जाती है "? इस प्रकार का हमला उस व्यवस्थापक का लाभ उठाता है जो केवल बातें बनाना चाहता है उपयोगकर्ताओं के लिए जितना संभव हो उतना आसान। शायद ऐसा करने के लिए, व्यवस्थापक छोड़ देगा न्यूनतम संभव स्तर पर सुरक्षा सेटिंग्स, हर सेवा को सक्षम करें, और सभी फ़ायरवॉल पोर्ट खोलें। यह उपयोगकर्ताओं के लिए आसान है, लेकिन एक और सोना बनाता है हैकर के लिए मेरा।

EXAM TIP - Infowar (जैसा कि ECC इसे कॉल करना पसंद करता है) आक्रामक और का उपयोग है रक्षात्मक तकनीक अपने विरोधी पर

लाभ पैदा करने के लिए। परिभाषित प्रकृति में कौन से कार्य आक्रामक बनाम रक्षात्मक हैं, इसलिए सेल्फप्लेनेटरी होना चाहिए, इसलिए यदि आपसे पूछा जाए, तो सामान्य ज्ञान और तर्क का उपयोग करें। के लिये उदाहरण के लिए, आपके सिस्टम पर एक बैनर जो आपको पहुँच का प्रयास करने की चेतावनी देता है अभियोग प्रकृति में रक्षात्मक है, एक निवारक के रूप में कार्य करना।

Hacking Phases

हमलावर की मंशा के बावजूद (याद रखें कि अच्छे लोग हैं और बुरे लोग), हैकिंग और अटैकिंग सिस्टम कभी–कभी पायलट के समान हो सकते हैं और उसका विमान। यह सही है, मैंने उससे कहा। मेरी बेटी एक खोज और बचाव ह अमेरिकी वायु सेना के लिए हेलीकॉप्टर पायलट, और इस अल्ट्रा–कूल एक्सेस के कारण, मैं पायलटों के साथ समय–समय पर बात करना। मैं अक्सर उन्हें कहता सुनता हूं, जब एक मिशन या घटना के बारे में बताते हुए कि वे सिर्फ विमान को महसूस करते थे या हेलीकॉप्टर–कि वे सिर्फ जानते थे कि यह कैसा लग रहा था और सबसे अच्छी बात है कभी–कभी बिना सोचे–समझे भी लक्ष्य को पूरा करें। मैं थोड़ी देर पहले अपनी बेटी से बात कर रहा था और उससे इस बारे में पूछा मानव–मशीन संबंध। वह एक पल के लिए रुक गई और मुझसे कहा कि पक्का, यह मौजूद है, और यह सोचना अज्ञानता है कि पायलट ए ने एक शानदार निर्णय में एक्शन बी क्यों किया। हालांकि, उसने चेतावनी दी, वह सब रहस्यमय सामग्री कभी नहीं हो सकती सभी अप–फ्रंट प्रशिक्षण, समय और प्रक्रियाओं के बिना होता है। क्यों कि पायलटों ने एक प्रक्रिया का पालन किया और निर्णय लेने में अपना समय लगा दिया और मशीन के लगने से फल आने लगता है।

हैकिंग चरण, जैसा कि ईसी–काउंसिल द्वारा पहचाना जाता है, सोचने का एक शानदार तरीका है आपके लिए एक हमले की

संरचना के बारे में, मेरे हैकिंग पायलट प्रशिक्षु। मैं नही कह रहा हूँ जब वे खुद को प्रस्तुत करते हैं तो आपको अवसरों का लाभ नहीं उठाना चाहिए सिर्फ इसलिए कि वे क्रम से बाहर हैं (यदि कोई मशीन स्वेच्छा से प्रस्तुत करती है और आप हमले से इनकार करते हुए कहते हैं, "लेकिन मैंने इसे अभी तक दोबारा नहीं जोड़ा है!" मैं रख सकता हूँ अपने आप को थप्पड़ मारने के लिए), लेकिन सामान्य तौर पर योजना के बाद गुणवत्ता का उत्पादन होगा परिणाम है। हालांकि इन चरणों और कुछ के लिए कई अलग–अलग शब्द हैं ईसी–काउंसिल के पास एक परीक्षण के दौरान, लगातार और लगातार चलाते हैं चित्रा 1-7 में दिखाया गया है, पाँच चरणों के रूप में मानक हैक परिभाषित 1 निःशुल्क. चाहे हमलावर नैतिक या दुर्भावनापूर्ण हो, ये पांच चरण पूर्ण पर कब्जा करते हैं हमले की चौड़ाई।

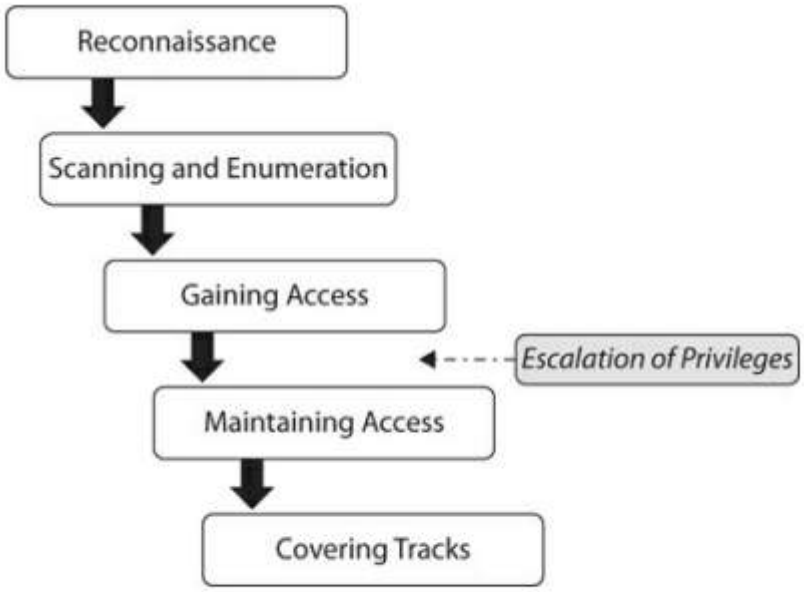


Figure 1-7 Phases of ethical hacking

EXAM TIP - आपके अध्ययन के दौरान हैकिंग के चरणों को ध्यान में रखें। आप सबसे अधिक संभावना है कि कई सवाल पूछेंगे कि आप न केवल पहचान सकते हैं प्रत्येक चरण में होता है लेकिन कौन से उपकरण प्रत्येक में उपयोग किए जाते हैं।

टोही शायद सबसे कठिन चरण होने जा रहा है Exam के लिए समझना, मुख्य रूप से क्योंकि बहुत से लोग इसके कुछ को भ्रमित करते हैं अगले चरण का हिस्सा होने के रूप में कदम (स्कैनिंग और गणना)। साक्ष्य इकट्ठा करने के लिए उठाए गए कदमों से ज्यादा कुछ भी नहीं है उन लक्ष्यों की जानकारी जिन पर आप हमला करना चाहते हैं। यह प्रकृति में निष्क्रिय हो सकता है या सक्रिय। निष्क्रिय टोही में आपके बारे में जानकारी एकत्र करना शामिल है उनके ज्ञान के बिना लक्ष्य, जबकि सक्रिय टोही उपकरण और का उपयोग करता है ऐसी तकनीकें जो खोजी जा सकती हैं या नहीं लेकिन अपनी गतिविधियों को एक के रूप में रखें खोज के अधिक जोखिम में हैकर।

इसके बारे में सोचने का एक और तरीका है नेटवर्क परिप्रेक्ष्य: सक्रिय वह है जो उद्देश्यपूर्ण तरीके से पैकेट डालता है, या विशिष्ट संचार, आपके लक्ष्य के लिए एक तार पर, जबकि निष्क्रिय नहीं करता है। उदाहरण के लिए, अपने प्रवेश Exam की कल्पना करें, जिसे पेन टेस्ट भी कहा जाता है बस शुरू किया और आपको पता है कि आप जिस कंपनी को लक्षित कर रहे हैं, उसके बारे में कुछ भी नहीं है। निष्क्रिय रूप से, आप केवल एक जोड़े के लिए भवन के बाहर देख सकते हैं कर्मचारी की आदतों को जानने और शारीरिक सुरक्षा उपायों के बारे में जानने के लिए दिन स्थान। सक्रिय रूप से, आप बस प्रवेश द्वार या गार्ड झोंपड़ी तक चल सकते हैं और दरवाजा (या गेट) खोलने का प्रयास करें। किसी भी मामले में, आप मूल्यवान सीख रहे हैं जानकारी, लेकिन निष्क्रिय टोही के साथ आप कोई कार्रवाई नहीं कर रहे हैं दूसरों को संकेत दें कि आप देख रहे हैं। कार्यों के उदाहरण जो हो सकते हैं।

इस चरण के दौरान सोशल इंजीनियरिंग, डंपस्टर डाइविंग और

नेटवर्क हैं।

sniffing – इस अध्ययन के शेष के दौरान सभी संबोधित कर रहे हैं मार्गदर्शक। ध्यान दें कि ग्रह पर हर पेन परीक्षक जो एक डंपर में घुटने से गहरा हो उनके चेहरे में एक गार्ड की टॉर्च के साथ पता है कि डंपस्टर डाइविंग के रूप में है एक आयरनमैन ट्रायथलॉन चलाने के रूप में एक गतिविधि। बस इतना ध्यान रखें कभी–कभी परिभाषाएँ और वास्तविकता मेल नहीं खातीं। अपने Exam के लिए, यह है निष्क्रिय। वास्तविक जीवन में, यह एक बड़ा जोखिम है, और आप शायद बदबू मारेंगे।

दूसरे चरण में, स्कैनिंग और एन्यूमरेशन, सुरक्षा पेशेवर वे जानकारी को संकलित करें और सक्रिय रूप से उपकरण लागू करें और लक्ष्यों पर अधिक गहराई से जानकारी इकट्ठा करने की तकनीक। यह हो सकता है देखने के लिए पिंग स्वीप या नेटवर्क मैपर चलाने जैसा ही कुछ सरल है क्या सिस्टम नेटवर्क पर हैं, या एक Vulnerability चलाने के रूप में जटिल है यह निर्धारित करने के लिए कि कौन से पोर्ट किसी सिस्टम पर खुले हो सकते हैं। के लियेउदाहरण के लिए, जबकि सामंजस्य ने नेटवर्क को 500 या तो दिखाया होगा एक इमारत, स्कैनिंग और के अंदर एक ही सबनेट से जुड़ी मशीनें गणन आपको बताएगा कि कौन सी विंडोज मशीनें हैं और कौन सी हैं लोग एफ़टीपी चला रहे हैं।

तीसरा चरण, जैसा कि वे कहते हैं, जहां जादू होता है। यह चरण है अधिकांश लोग खुशी से उल्लास में घूमते हुए अपने हाथों को एक साथ रगड़ते हैं उन्हें पता है कि वे एक सुरक्षा नियंत्रण को दरकिनार करके प्राप्त करेंगे। पाने में पहुँच चरण, सही हमलों में निर्धारित लक्ष्यों के खिलाफ लगाए गए हैं दूसरा चरण। ये हमले एक खुले और तक पहुँचने के रूप में सरल हो सकते हैं बेतार वायरलेस

एक्सेस बिंदु और फिर जो भी इसके लिए हेरफेर करना उद्देश्य, या बफर ओवरफ्लो या एसक्यूएल लिखने और वितरित करने के रूप में जटिल एक वेब अनुप्रयोग के खिलाफ इंजेक्शन। में इस्तेमाल किए जाने वाले हमले और तकनीक इस अध्ययन गाइड के शेष भाग में चरण पर चर्चा की जाएगी।

चौथे चरण में, पहुंच को बनाए रखते हुए, हैकर्स उन्हें सुनिश्चित करने का प्रयास करते हैं मशीन या सिस्टम में वे पहले से ही समझौता कर चुके हैं। भविष्य के उपयोग के लिए हमलावर द्वारा पिछले दरवाजे खुले छोड़ दिए जाते हैं, खासकर यदि प्रणाली को एक ज़ोंबी (लॉन्च करने के लिए इस्तेमाल की जाने वाली मशीन) में बदल दिया गया है आगे के हमले) या यदि सिस्टम का उपयोग आगे की सूचना एकत्र करने के लिए किया जाता है – उदाहरण के लिए, एक स्निफर को देखने के लिए एक समझौता मशीन पर रखा जा सकता है एक विशिष्ट सबनेट पर यातायात। के उपयोग के माध्यम से पहुंच को बनाए रखा जा सकता है ट्रोजन, रूटकिट, या अन्य तरीकों की संख्या।

ध्यान दें कि मैंने पहले और वसीयत में उल्लेख किया है कि एक महत्वपूर्ण अंतर है इस पुस्तक के माध्यम से बार–बार उल्लेख: ईसीसी और के लिए अध्ययन सामग्री वास्तविक दुनिया और वास्तविक हैकिंग के साथ CETentimes का उतना ही लेना–देना है परमाणु संलयन के रूप में डोनट शीशा लगाना है। उदाहरण के लिए, वास्तविक में दुनिया, कलम परीक्षक और हैकर्स केवल स्कैनिंग और गणना करते हैं उपयोगी बुद्धि प्राप्त करने की संभावना जोखिम के मुकाबले अधिक है लक्ष्य द्वारा पता लगाना या प्रतिक्रिया करना। यकीन है, आप के रूप में ज्यादा जानकारी की जरूरत है आप सामने उठ सकते हैं, लेकिन अगर आप जो कर रहे हैं, वह अनावश्यक रूप से खींचने वाली हवाएं हैं अपने आप पर ध्यान दें,

पूरी बात व्यर्थ है। एक ही बात के लिए चला जाता है विशेषाधिकार वृद्धि: यदि आप वह कर सकते हैं जो आप चाहते हैं या बिना आवश्यकता के जड़ विशेषाधिकार को बढ़ाने के लिए परेशान, हुजह!

अंतिम चरण में, पटरियों को कवर करते हुए, हमलावर अपने को छुपाने का प्रयास करते हैं सफलता और सुरक्षा पेशेवरों द्वारा पता लगाने से बचें। यहां उठाए गए कदम छिपी हुई विशेषताओं के साथ फ़ाइलों को छुपाना या लॉग फ़ाइलों को हटाना या बदलना शामिल है निर्देशिका, और यहां तक कि के साथ संवाद करने के लिए सुरंग प्रोटोकॉल का उपयोग करना प्रणाली। यदि ऑडिटिंग चालू है और निगरानी की जाती है, और अक्सर यह नहीं है, तो फ़ाइलों को लॉग करें एक मशीन पर हमलों का एक संकेतक है। लॉग फ़ाइल को पूरी तरह से साफ़ करना मशीन को देखने वाले सुरक्षा व्यवस्थापक के लिए बस इतना बड़ा संकेतक, इसलिए कभी–कभी चयनात्मक संपादन आपका सबसे अच्छा दांव होता है। उपयोग करने के लिए एक और बढ़िया तरीका यहाँ केवल लॉग फ़ाइल को दूषित कर रहा है – जबकि पूरी तरह से खाली लॉग फ़ाइल चिल्लाती है एक हमले प्रगति पर है, फाइलें हर समय दूषित हो जाती हैं, और, संभावना है, व्यवस्थापक इसे फिर से बनाने की कोशिश कर परेशान नहीं करेगा। किसी भी स्थिति में, अच्छे पेन परीक्षक वास्तव में इस चरण में परिभाषित किए गए हैं।

नोट जब यह लॉग को दूषित या हटाने की बात आती है तो वास्तव में सावधान रहें असली दुनिया। एक कलम परीक्षक के रूप में आप एक "कोई नुकसान नहीं" खंड से बंधे होते हैं, जो आपको लॉग फ़ाइलों को बिल्कुल बदलने से रोक देगा। इतना ही नहीं कारण होगा संगठन को नुकसान पहुंचा सकता है, लेकिन उन्हें वास्तविक की खोज करने से भी रोक सकता है बुरे लोग जो आपके परीक्षण के दौरान हमला कर सकते हैं।

अंतर्दृष्टि के एक जोड़े को यहां प्राप्त किया जाना चाहिए और चाहिए। पहले, इसके विपरीत आम धारणा, पेन परीक्षक आमतौर पर उम्मीद से बेतरतीब ढंग से हमला नहीं करते हैं शोषण के लिए कुछ अनदेखी Vulnerability का पता लगाना। इसके बजाय, वे एक का पालन करें सिस्टम के हर पहलू को अच्छी तरह से जानने के लिए विशिष्ट, संगठित विधि वे निशाना लगा रहे हैं। पेन टेस्ट करने वाले अच्छे एथिकल हैकर्स ये सुनिश्चित करते हैं कदम बहुत अच्छी तरह से प्रलेखित हैं, असाधारण और विस्तृत नोट्स और अंतिम रूप में शामिल करने के लिए स्क्रीनशॉट और लॉग फाइल जैसी वस्तुओं को रखना रिपोर्ट good। श्री होर्टन, हमारे प्रिय तकनीकी संपादक, इसे इस तरह से रखें: पेन परीक्षक ग्राहक के लिए अपने काम में पूरी तरह से लगे हैं। हैकर्स को बस पता चलता है कि क्या है अपने लक्ष्य को पूरा करने के लिए आवश्यक है। दूसरा, सुरक्षा का ध्यान रखें।

पेन टेस्ट करने वाले पेशेवर आम तौर पर किसी की मरम्मत या पैचअप नहीं करते हैं सुरक्षा कमजोरियाँ जो वे पाते हैं – ऐसा करना उनका काम नहीं है। एथिकल हैकर का काम ग्राहक के लिए सुरक्षा खामियों की खोज करना है, न कि उसे ठीक करना उन्हें। पुल को उड़ाने का तरीका जानने से आप सिविल इंजीनियर नहीं बन जाते एक निर्माण में सक्षम है, तो जबकि आपके अनुकूल पड़ोस CEH हो सकता है अपनी समस्याओं को खोजने में सक्षम, यह किसी भी तरह से गारंटी नहीं देता है कि वह इंजीनियर बन सकता है सुरक्षित प्रणाली।

नोट - कोई हैकर जो किसी विशेष के बाद है चिपके हुए परेशान नहीं कर सकता है जो चाहता है उसे पाने के लिए एक निर्धारित विधि। असली दुनिया में हैकर्स होगा

अंतिम लक्ष्य के लिए सबसे आसान, तेज, सरल मार्ग का लाभ उठाएं, और यदि इसका मतलब है कि एनुमरेट करने से पहले हमला करना, फिर ऐसा होना।

The Ethical Hacker

तो] क्या किसी को "नैतिक" हैकर बनाता है? क्या ऐसा भी हो सकता है? हैकिंग कंप्यूटर और सिस्टम की कला को ध्यान में रखते हुए, अपने आप में, ए गुप्त कार्रवाई, ज्यादातर लोगों का मानना है कि एक निकट संबंधी गतिविधि में उलझने के बारे में सोचा जाना अनैतिक होगा। हालांकि, उद्देश्य और अधिनियम के इरादे को ध्यान में रखा जाना चाहिए।

तुलना के लिए, कानून प्रवर्तन पेशेवर नियमित रूप से भाग लेते हैं अनैतिक व्यवहार और स्थितियों में बेहतर समझने के लिए, और करने के लिए पकड़, उनके आपराधिक समकक्षों। पुलिस और एफबीआई एजेंटों को लिंगो को सीखना चाहिए, कार्रवाई, और दवा कार्टेल और संगठित अपराध के व्यवहार घुसपैठ और अपराधियों का भंडाफोड़, और ऐसा करना कभी–कभी उन्हें मजबूर करता है खुद आपराधिक कृत्य में लिप्त। एथिकल हैकिंग के बारे में सोचा जा सकता है उसी तरह। एक में Vulnerability और सुरक्षा छेद को खोजने और ठीक करने के लिए कंप्यूटर सिस्टम या नेटवर्क, आपको कभी–कभी एक अपराधी की तरह सोचना पड़ता है और उसी रणनीति, उपकरण और प्रक्रियाओं का उपयोग करें जो वे नियोजित कर सकते हैं। सीईएच पार्लेंस में, और कई अन्य संस्थाओं द्वारा परिभाषित के रूप में, ए है एक हैकर और एक पटाखा के बीच अंतर। एथिकल हैकर है कोई व्यक्ति जो एक ही उपकरण और तकनीकों को नियुक्त करता है वह एक अपराधी का उपयोग कर सकता है, नेटवर्क को सुरक्षित करने में मदद करने के लिए ग्राहक के पूर्ण समर्थन और अनुमोदन के साथ प्रणाली। एक पटाखा, जिसे एक दुर्भावनापूर्ण हैकर के रूप में भी

जाना जाता है, उन कौशल, उपकरणों का उपयोग करता है, और तकनीक व्यक्तिगत लाभ या विनाशकारी उद्देश्यों के लिए या, विशुद्ध रूप से तकनीकी शब्द, सिस्टम के मालिक के हित के बाहर एक लक्ष्य को प्राप्त करने के लिए। एथिकल हैकर्स सुरक्षा में सुधार के लिए ग्राहकों द्वारा नियोजित किए जाते हैं। पटाखे या तो अपने दम पर काम करते हैं या, कुछ मामलों में, नष्ट करने के लिए या किराए पर एजेंटों के रूप में कार्य करते हैं सरकार या कॉर्पोरेट प्रतिष्ठा को नुकसान।

हैकर को नैतिक बनाम बैडगी क्रैकर्स के रूप में पहचानने वाले सभी महत्वपूर्ण विशिष्टों को बार–बार हाइलाइट किया जाना चाहिए। एथिकल हैकर्स के बीच बनी सहमति के दायरे में काम करते हैं किसी भी कार्रवाई से पहले खुद और एक ग्राहक। यह समझौता नहीं है बस एक मुस्कान, एक वार्तालाप, और एक हैंडशेक के ठीक पहले आप एक फ्लिप खोलते हैं लैपटॉप और दूर हैकिंग शुरू। नहीं, इसके बजाय यह सावधानीपूर्वक रखी गई योजना है, एथिकल हैकर और दोनों की रक्षा करने के लिए सावधानीपूर्वक व्यवस्था और दस्तावेज किया गया है ग्राहक।

सामान्य तौर पर, एक एथिकल हैकर पहले क्लाइंट के साथ बैठक करेगा और हस्ताक्षर करेगा अनुबंध। अनुबंध न केवल अनुमति और प्राधिकरण को परिभाषित करता है सुरक्षा पेशेवर को दिया जाता है (जिसे कभी–कभी जेल–से–मुक्त कहा जाता है कार्ड) लेकिन यह भी गोपनीयता और गुंजाइश। कोई भी ग्राहक कभी होने के लिए सहमत नहीं होगा हैकर सुनिश्चित करने के बिना सुरक्षा को भंग करने का एक नैतिक हैकर का प्रयास परीक्षण के दौरान मिली किसी भी जानकारी का खुलासा नहीं करेगा। आमतौर पर, यह चिंता एक गैर–प्रकटीकरण समझौते (एनडीए) के निर्माण में परिणाम।

इसके अतिरिक्त, ग्राहक लगभग हमेशा चाहते हैं कि परीक्षण एक निश्चित प्रक्रिया के लिए आगे बढ़े नेटवर्क संरचना में बिंदु और आगे नहीं: "आप के माध्यम से प्राप्त करने की कोशिश कर सकते हैंफ़ायरवॉल, लेकिन दूसरी ओर फ़ाइल सर्वरों को स्पर्श न करें ... क्योंकि तुम हो सकता है।

मेरे एमपी 3 संग्रह को परेशान।"वे यह भी प्रतिबंधित करना चाहते हैं कि किस प्रकार का आपके द्वारा चलाए गए हमले। उदाहरण के लिए, क्लाइंट आपके साथ पूरी तरह से ठीक हो सकता है उनके सिस्टम के खिलाफ एक पासवर्ड हैक करने का प्रयास किया जा सकता है लेकिन आप नहीं चाहते हैं आप जानते हैं कि हर DoS हमले का परीक्षण करें।

हालांकि, भले ही आप अपनी सुरक्षा का परीक्षण करने के लिए काम पर रखे गए हों आप जानते हैं कि सुरक्षा और हैकिंग हलकों में वास्तव में क्या महत्वपूर्ण है एक लक्ष्य के लिए गंभीर जोखिमों को "महत्वपूर्ण" होने के कारण परीक्षण करने की अनुमति नहीं हैसंसाधन का।" यह] वैसे, अक्सर कॉर्पोरेट ट्रस्ट का एक कार्य होता हैकलम परीक्षक और संगठन के बीच और समय के साथ बदलाव होगा; क्या है आज के परीक्षण में महत्वपूर्ण संसाधन जांच और "चलो देखते हैं क्या होता है "अगले साल। यदि परीक्षण वास्तव में सुरक्षा में सुधार करने के लिए डिज़ाइन किया गया है एक सर्वर को उड़ा देता है, यह एक विजयी परिदृश्य नहीं हो सकता है; हालाँकि, कभी–कभी डेटा जो वास्तव में जोखिम में है, यह आगे बढ़ने के लिए महत्वपूर्ण है। यह सचमुच सुरक्षा परीक्षण वार्ता के दौरान शांत और केंद्रित दिमाग में उबाल आता है।

ध्यान दें कि आपके CEH अध्ययन में संदर्भित सामान्य शब्द बाघ है

टीम, जो लोगों के एक समूह से ज्यादा कुछ नहीं है, एक साथ एकत्र हुए व्यापार इकाई, किसी विशिष्ट समस्या या लक्ष्य को संबोधित करने के लिए काम करना। नैतिक हैकर्स कभी–कभी एक बाघ टीम का हिस्सा होते हैं, जो सभी पहलुओं को अच्छी तरह से परखने के लिए तैयार किए जाते हैं एक सुरक्षा प्रणाली की। चाहे आप टीम के हिस्से के रूप में रखे गए हों या ए के रूप में व्यक्तिगत, सगाई के नियमों पर ध्यान दें।

The Pen Test

कंपनियों और सरकारी एजेंसियों के विभिन्न प्रकार के लिए प्रवेश परीक्षण के लिए पूछना कारणों। कभी–कभी नियम और कानून इस मुद्दे को बल देते हैं। उदाहरण के लिए, कई चिकित्सा सुविधाओं को स्वास्थ्य बीमा के अनुपालन को बनाए रखने की आवश्यकता है पोर्टेबिलिटी एंड एकाउंटेबिलिटी एक्ट (HIPAA) और एथिकल हैकर्स को किराए पर देगा उनकी मान्यता पूरी करें। कभी–कभी संगठन का नेतृत्व होता है बस सुरक्षा के प्रति जागरूक और जानना चाहता है कि मौजूदा सुरक्षा कितनी अच्छी है नियंत्रण कार्य कर रहे हैं। और कभी–कभी यह केवल विश्वास के पुनर्निर्माण का प्रयास होता है और सुरक्षा भंग के बाद प्रतिष्ठा पहले से ही हुई है। यह एक बात है ग्राहकों को बताएं कि आपने सुरक्षा दोष को ठीक कर लिया है जिसने सभी की चोरी की अनुमति दी है पहली बार में उन क्रेडिट कार्ड। यह दिखाने के लिए पूरी तरह से एक और बात है नए नियंत्रण के खिलाफ एक प्रवेश Exam के परिणाम।

एक नैतिक हैकर के रूप में आपकी Exam और आपके भविष्य के संबंध में, वहाँ हैं दो प्रक्रियाओं को आपको जानना होगा: कैसे सेट अप करें और एक कानूनी प्रदर्शन करें पैठ परीक्षण और वास्तविक हैक के माध्यम से कैसे आगे बढ़ना है। एक पैठ परीक्षण एक प्रणाली की सुरक्षा नियंत्रणों का स्पष्ट रूप से परिभाषित, पूर्ण पैमाने पर

परीक्षण है सुरक्षा जोखिमों और कमजोरियों की पहचान करने के लिए नेटवर्क और तीन हैं प्रमुख चरण। एक बार पेन टेस्ट पर सहमति हो जाने के बाद, एथिकल हैकर शुरू होता है विभिन्न प्रकार के उपकरणों, विधियों और तकनीकों का उपयोग करके "हमला", लेकिन आम तौर पर परीक्षण करने के लिए एक विशिष्ट हैक के समान पाँच चरणों का अनुसरण करता है। के लिए सीईएच Exam, आपको तीन पेन परीक्षण चरणों और से परिचित होना होगा एक ठेठ हैक के पांच चरणों।

एक पेन टेस्ट के तीन मुख्य चरण होते हैं– तैयारी, मूल्यांकन और निष्कर्ष – और वे परिभाषित करने और समझने में काफी आसान हैं। तैयारी चरण उस समयावधि को परिभाषित करता है जिसके दौरान वास्तविक अनुबंध होता है बाहर अंकित। परीक्षण का दायरा, हमलों के प्रकार की अनुमति है, और गतिविधि करने के लिए सौंपे गए व्यक्ति इस चरण में सभी सहमत हैं।

मूल्यांकन चरण (कभी–कभी सुरक्षा मूल्यांकन के रूप में भी जाना जाता है चरण या चालन चरण) ठीक वैसा ही है जैसा लगता है – वास्तविक हमले इस दौरान सुरक्षा नियंत्रण आयोजित किए जाते हैं। अंत में, निष्कर्ष (या मूल्यांकन के बाद का चरण उस समय को परिभाषित करता है जब अंतिम रिपोर्ट तैयार की जाती है ग्राहक के लिए, परीक्षणों के निष्कर्षों का विवरण (प्रकार सहित) परीक्षण किए गए) और कई बार सिफारिशें भी प्रदान करते हैं

सुरक्षा में सुधार। एक कलम परीक्षण करने में, एक नैतिक हैकर को प्रतिबिंबित करने का प्रयास करना चाहिए जितना संभव हो आपराधिक दुनिया। दूसरे शब्दों में, अगर कदम उठाए गए हैं पेन टेस्ट के दौरान एथिकल हैकर पर्याप्त रूप से आईना नहीं दिखाता कि असली क्या है? हैकर करेगा, तो परीक्षण विफलता के लिए बर्बाद

है। उस कारण से, सबसे कलम परीक्षणों में लक्ष्य के बारे में ज्ञान के विभिन्न चरणों में अभिनय करने वाले व्यक्ति होते हैं मूल्यांकन (टीओई)। इन विभिन्न प्रकार के परीक्षणों को तीन नामों से जाना जाता है:

ब्लैक बॉक्स, व्हाइट बॉक्स और ग्रे बॉक्स।
ब्लैक–बॉक्स परीक्षण में, एथिकल हैकर को इसके बारे में बिल्कुल जानकारी नहीं है पैर की अंगुली। यह एक बाहरी, अज्ञात हमलावर का अनुकरण करने के लिए डिज़ाइन किया गया है, और यह लेता है समय की पूरी राशि और, आमतौर पर, अब तक सबसे महंगी है विकल्प। एथिकल हैकर के लिए, ब्लैक–बॉक्स परीक्षण का मतलब पूरी तरह से रोमांटिक है एक हमले के पांच चरणों के माध्यम से और के किसी भी पूर्व धारणा को हटा देता है क्या देखें। इस प्रकार के परीक्षण में एकमात्र सही दोष यह ध्यान केंद्रित है केवल संगठन के बाहर खतरे पर और ध्यान में नहीं लेता है किसी भी विश्वसनीय उपयोगकर्ता अंदर पर।

नोट - एक महत्वपूर्ण वास्तविक दुनिया बनाम परिभाषा भेद यहां उत्पन्न होता है: जबकि इस शब्द की शुद्ध परिभाषा में कोई ज्ञान नहीं है, एक ब्लैक–बॉक्स टेस्ट है यह देखने के लिए डिज़ाइन किया गया है कि बाहरी हैकर के पास क्या है और पहले के बारे में जानता है हमला शुरू करना। निश्चिंत रहें, बुरे लोग चीजों पर शोध कर रहे हैं एक लम्बा समय। वे कुछ जानते हैं या वे पहली जगह पर हमला नहीं करेंगे।

एक कलम परीक्षक के रूप में, आपको बेहतर होगा कि आप उन्हीं चीजों से अवगत हों, जब वे होती हैं अपना परीक्षण स्थापित करना।

व्हाइट–बॉक्स परीक्षण ब्लैक–बॉक्स परीक्षण के बिल्कुल विपरीत है।

इस प्रकार में, पेन टेस्टर्स को नेटवर्क, सिस्टम और इन्फ्रास्ट्रक्चर की पूरी जानकारी होती है वे निशाना लगा रहे हैं। यह, काफी स्पष्ट रूप से, परीक्षण को बहुत तेज, आसान बनाता है, और कम खर्चीला, और यह एक आंतरिक आंतरिक अनुकरण करने के लिए डिज़ाइन किया गया है धमकी, जैसे कि एक असंतुष्ट नेटवर्क व्यवस्थापक या अन्य विश्वसनीय उपयोगकर्ता।

अंतिम प्रकार, ग्रे–बॉक्स परीक्षण, को आंशिक ज्ञान परीक्षण के रूप में भी जाना जाता है। यह ब्लैक–बॉक्स परीक्षण से अलग क्या है इसका मान लिया गया स्तर है परीक्षक के पास विशेषाधिकार हैं। जबकि ब्लैक–बॉक्स परीक्षण आम तौर पर होता है नेटवर्क प्रशासन स्तर से किया जाता है, ग्रे–बॉक्स परीक्षण केवल मानता है हमलावर एक अंदरूनी सूत्र है। क्योंकि ज्यादातर हमले एक के अंदर से उत्पन्न होते हैं नेटवर्क, इस प्रकार का परीक्षण मूल्यवान है और विशेषाधिकार प्रदर्शित कर सकता है एक विश्वसनीय कर्मचारी से वृद्धि।

कानून और मानक

अंत में, यदि आप अपने आप को एक नैतिक कुछ भी कहना असंभव होगा दिशानिर्देशों, मानकों और कानूनों को नहीं समझते जो आपके शासन करते हैं विशेषज्ञता का विशेष क्षेत्र। आईटी सुरक्षा के हमारे दायरे में (और नैतिक में) हैकिंग), ऐसे कई कानून और मानक हैं जिनसे आपको परिचित होना चाहिए केवल एक अच्छा काम करने के लिए, लेकिन आपको परेशानी और जेल से बाहर रखने के लिए। हम थे Exam के पिछले संस्करणों में भाग्यशाली है कि ये बहुत बार हिट नहीं हुए, लेकिन अब वे वापस आ गए हैं – और प्रतिशोध के साथ।

मुझे वादा करना अच्छा लगेगा कि मैं आपको एक व्यापक सूची प्रदान कर सकता हूं कानून आपको अपनी नौकरी के लिए जानने की आवश्यकता होगी, लेकिन अगर मैंने किया तो यह पुस्तक आकार

होगा एक पुराने विश्वकोश और आप इसे कभी नहीं खरीदेंगे। आपके लिए बहुत सारे कानून हैं अपनी नौकरी के लिए जागरूक होने की जरूरत है, जैसे कि FISMA, इलेक्ट्रॉनिक्स संचार गोपनीयता अधिनियम, पैट्रियट अधिनियम, 1974 का गोपनीयता अधिनियम, साइबर इंटेलिजेंस शेयरिंग एंड प्रोटेक्शन एक्ट (CISPA), उपभोक्ता डेटा सुरक्षा और अधिसूचना अधिनियम, 1987 का कंप्यूटर सुरक्षा अधिनियम...सूची वास्तव में है लगभग अंतहीन। चूंकि यह आपको राज्य बार Exam के लिए तैयार करने के लिए कोई पुस्तक नहीं है, मैं इन सभी को परिभाषित नहीं करने जा रहा हूं। अध्ययन के लिए, और रखते हुए मेरा पृष्ठ कुछ हद तक नीचे गिना जाएगा, हम बस कुछ चर्चा करेंगे जो आपको चाहिए परीक्षण के उद्देश्यों पर ध्यान केंद्रित करें – क्योंकि वे ईसीसी वाले हैं इस गो–राउंड को करीब से देख रहे हैं। जब तुम असली में निकलते हो दुनिया, आपको सीखने और जानने की आवश्यकता होगी, बाकी।

सबसे पहले स्वास्थ्य बीमा पोर्टेबिलिटी और जवाबदेही अधिनियम है (HIPAA), अमेरिकी स्वास्थ्य और मानव सेवा विभाग द्वारा विकसित किया गया है चिकित्सा जानकारी के संबंध में गोपनीयता मानकों को संबोधित करने के लिए। कानून सेट करता है रोगी के मेडिकल रिकॉर्ड और स्वास्थ्य जानकारी की सुरक्षा के लिए गोपनीयता मानक, जो, डिज़ाइन द्वारा, डॉक्टरों, अस्पतालों और बीमा को प्रदान और साझा किया जाता है प्रदाताओं। HIPAA के पांच उपखंड हैं जो काफी आत्म–व्याख्यात्मक हैं
(इलेक्ट्रॉनिक लेनदेन और कोड सेट, गोपनीयता नियम, सुरक्षा नियम, राष्ट्रीय पहचानकर्ता आवश्यकताएँ, और प्रवर्तन) और आपकी Exam में दिखाई दे सकती हैं।

आपके अध्ययन के लिए एक और महत्वपूर्ण कानून सरबेंस–ऑक्सले

(एसओएक्स) अधिनियम है। SOX को कॉर्पोरेट खुलासे को अधिक सटीक और विश्वसनीय बनाने के लिए बनाया गया था जनता और निवेशकों को छायादार व्यवहार से बचाने के लिए। 11 हैं SOX के भीतर शीर्षक जो सब कुछ संभालते हैं कि वित्तीय क्या होना चाहिए की ऑडिटर संघर्षों से रक्षा करने के लिए, रिपोर्ट की गई और उनमें क्या जाना चाहिए जवाबदेही के लिए ब्याज और प्रवर्तन।

नोट - एक बात जो आपको बेहतर सुरक्षा स्थापित करने में मदद कर सकती है वह है OSSTM – ओपन सोर्स सिक्योरिटी टेस्टिंग मेथोडोलॉजी मैनुअल (यदि आप वास्तव में चाहते हैं डरावना ध्वनि करने के लिए, इसे "एक स्टेम" कहें. यह एक सहकर्मी की समीक्षा औपचारिक है सुरक्षा परीक्षण और विश्लेषण की कार्यप्रणाली जो "कार्रवाई योग्य प्रदान कर सकती है।" आपके परिचालन सुरक्षा में सुधार करने के लिए जानकारी।"यह परिभाषित करता है परीक्षण के लिए तीन प्रकार के अनुपालन: विधायी (सरकारी नियम)), संविदात्मक (उद्योग या समूह की आवश्यकताएं), और मानक आधारित (प्रथाओं) किसी समूह का सदस्य बने रहने के लिए इसका पालन किया जाना चाहिए संगठन)।

जब मानकों की बात आती है, तो फिर से जानने के लिए टन होते हैं – शायद नहीं अपनी नौकरी के लिए जरूरी है, लेकिन क्योंकि आप उन्हें इस Exam में देखेंगे। एक जोड़ा ECC वास्तव में आपको जानना चाहता है कि PCI–DSS और ISO / IEC हैं27001:2013. भुगतान कार्ड उद्योग डेटा सुरक्षा मानक (PCI–DSS) एक सुरक्षा है क्रेडिट कार्ड, एटीएम कार्ड और अन्य पॉइंट–सेल्स कार्ड से निपटने वाले संगठनों के लिए मानक। मानकों में शामिल सभी समूहों और संगठनों पर लागू होता है भुगतान प्रक्रिया की संपूर्णता में– कार्ड जारी करने वालों से लेकर व्यापारियों तक

उन भंडारण और संचारण कार्ड जानकारी – और 12 से मिलकर बनता है आवश्यकताओं:

- आवश्यकता 1: रक्षा करने के लिए फ़ायरवॉल कॉनफ़िगरेशन स्थापित और बनाए रखें डेटा।
- आवश्यकता 2: विक्रेता द्वारा प्रदत्त डिफ़ॉल्ट पासवर्ड और अन्य को हटा दें डिफ़ॉल्ट सुरक्षा सुविधाएँ।
- आवश्यकता 3: संग्रहीत डेटा को सुरक्षित रखें।
- आवश्यकता 4: कार्डधारक डेटा के प्रसारण को एनक्रिप्ट करें।
- आवश्यकता 5: एवी (एंटीवायरस) को इंस्टॉल, उपयोग और अपडेट करें।
- आवश्यकता 6: सुरक्षित सिस्टम और एप्लिकेशन विकसित करें।
- आवश्यकता 7: पहुँच को प्रतिबंधित करने के लिए दिशानिर्देश के रूप में "जानने की आवश्यकता" का उपयोग करें डेटा।
- आवश्यकता 8: प्रक्रिया में प्रत्येक हितधारक को एक अद्वितीय आईडी असाइन करें (कंप्यूटर एक्सेस के साथ)।
- आवश्यकता 9: डेटा तक किसी भी भौतिक पहुँच को प्रतिबंधित
- आवश्यकता10: डेटा और नेटवर्क संसाधनों तक सभी पहुंच की निगरानी करें धारण करना, संचार करना या उसकी रक्षा करना।
- आवश्यकता 11: नियमित रूप से सुरक्षा प्रक्रियाओं और प्रणालियों का परीक्षण करें।
- आवश्यकता12: सूचना सुरक्षा नीति बनाएं और बनाए रखें।

सूचना और संबंधित प्रौद्योगिकी (COBIT) के लिए नियंत्रण ऑब्जेक्ट है

एक और सुरक्षा मानक जिसे आप शायद संदर्भित देखेंगे। द्वारा बनाया गया सूचना प्रणाली लेखा Exam और नियंत्रण संघ (ISACA) और आईटी
गवर्नेंस इंस्टीट्यूट (ITGI), COBIT (ISACA की अपनी वेबसाइट से) है, "एक IT शासन की रूपरेखा और सहायक टूलसेट जो प्रबंधकों को पुल करने की अनुमति देता है नियंत्रण आवश्यकताओं, तकनीकी मुद्दों और व्यावसायिक जोखिमों के बीच की खाई। COBIT स्पष्ट नीति विकास, अच्छा अभ्यास और जोर देने में सक्षम बनाता है नियामक अनुपालन।" यह नियंत्रण उद्देश्यों को वर्गीकृत करके भाग में ऐसा करता है निम्नलिखित डोमेन में:

- योजना और संगठन
- अधिग्रहण और कार्यान्वयन
- वितरण और समर्थन
- जाचना और परखना

प्रत्येक डोमेन में विशिष्ट नियंत्रण उद्देश्य होते हैं। यह मानक मदद करता है सुरक्षा आर्किटेक्ट पता लगाते हैं और न्यूनतम सुरक्षा आवश्यकताओं की योजना बनाते हैं उनके संगठन।

और चाहिए? मैं या तो नहीं है, इसलिए मैं आपको एक अंतिम उदाहरण ईसीसी के साथ छोड़ दूँगा के बारे में परवाह करने के लिए लगता है: आईएसओ / आईईसी27001: 2013। यह आवश्यकताओं को प्रदान करता है संगठनात्मक आईएस (सूचना) का निर्माण, रखरखाव और सुधार
सुरक्षा प्रणालियां। मानक सभी प्रकार की चीजों को संबोधित करता है, जैसे कि सुनिश्चित करना आंतरिक सुरक्षा आवश्यकताओं को तैयार करने के साथ ही कानूनों का अनुपालन और उद्देश्य।

अंत में, ध्यान रखें कि सूचना सुरक्षा कानून मुश्किल चीजें हैं जब राष्ट्रीय सीमाओं की बात आती है। जबकि एक अमेरिकी को लागू करना आसान है संयुक्त राज्य अमेरिका की भौतिक सीमाओं के भीतर बीज बोने के बारे में नियम, उस कानून का अर्थ चीन, ऑस्ट्रेलिया या फ्रांस में कुछ भी नहीं है। जब यह आता है सूचना और इंटरनेट, हालांकि, चीजें मुश्किल हो जाती हैं। की जटिलताएँ अन्य देशों में कानूनों को केवल इस पुस्तक में या किसी भी तरह से व्याख्यायित नहीं किया जा सकता है अन्य। आपको अपने नियोक्ता और अपनी टीम के साथ कुछ समय बिताना होगा किसी भी चीज़ के परीक्षण से पहले आपको क्या सीखना चाहिए।

नोट - कुछ लोगों को सिर्फ एक बहुत ही सरल, स्पष्ट अवलोकन मत भूलना के बारे में मत सोचो: इंटरनेट वैश्विक है। आपके हैक करने के बीच का अंतर चीन की सरकार को निशाना बनाना और हैक करना दुर्घटनावश सरल हो सकता है IP पते में गलत नंबर लिखना। और जबकि ज्यादातर लोग मानते हैं ट्रैफ़िक दुर्भावनापूर्ण है यदि यह आपके सिस्टम को विशेष रूप से लक्षित करता है, तो कई इसे देख सकते हैं दुर्भावनापूर्ण के रूप में अगर यह सिर्फ आपके सिस्टम को स्थानांतरित करता है।

Questions

1. Which of the following would be the best example of a deterrent control?

A. A log aggregation system
B. Hidden cameras onsite
C. A guard posted outside the door
D. Backup recovery systems

2. Enacted in 2002, this U.S. law requires every Federal agency to implement information security programs, including significant reporting on compliance and accreditation. Which of the following is the best choice for this definition?

A. FISMA
B. HIPAA
C. NIST 800-53
D. OSSTM

3. Brad has done some research and determined a certain set of systems on his network fail once every ten years. The purchase price for each of these systems is $1200. Additionally, Brad discovers the administrators on staff, who earn $50 an hour, estimate five hours to replace a machine. Five employees, earning $25 an hour, depend on each system and will be completely unproductive while it is down. If you were to ask Brad for an ALE on these devices, what should he answer with?

A. $2075
B. $207.50
C. $120
D. $1200

4. An ethical hacker is hired to test the security of a business network. The CEH is given no prior knowledge of the network and has a specific framework in which to work, defining boundaries, nondisclosure agreements, and the completion date. Which of the following is a true statement?

A. A white hat is attempting a black-box test.
B. A white hat is attempting a white-box test.
C. A black hat is attempting a black-box test.
D. A black hat is attempting a gray-box test.

5. When an attack by a hacker is politically motivated, the hacker is said to be participating in which of the following?

A. Black-hat hacking

B. Gray-box attacks
C. Gray-hat attacks
D. Hactivism

6. Two hackers attempt to crack a company's network resource security. One is considered an ethical hacker, whereas the other is not. What distinguishes the ethical hacker from the "cracker"?

A. The cracker always attempts white-box testing.
B. The ethical hacker always attempts black-box testing.
C. The cracker posts results to the Internet.
D. The ethical hacker always obtains written permission before testing.

7. In which stage of an ethical hack would the attacker actively apply tools and techniques to gather more in-depth information on the targets?

A. Active reconnaissance
B. Scanning and enumeration
C. Gaining access
D. Passive reconnaissance

8. Which type of attack is generally conducted as an inside attacker with elevated privileges on the resources?

A. Gray box
B. White box
C. Black box
D. Active reconnaissance

9. Which of the following Common Criteria processes refers to the system or product being tested?

A. ST
B. PP
C. EAL
D. TOE

10. Your company has a document that spells out exactly what employees are allowed to do on their computer systems. It also defines what is prohibited and what consequences await those who break the rules. A copy of this document is signed by all employees prior to their network access. Which of the following best describes this policy?

    A. Information Security Policy
    B. Special Access Policy
    C. Information Audit Policy
    D. Network Connection Policy

11. Sally is a member of a pen test team newly hired to test a bank's security. She begins searching for IP addresses the bank may own by searching public records on the Internet. She also looks up news articles and job postings to discover information that may be valuable. What phase of the pen test is Sally working?

    A. Preparation
    B. Assessment
    C. Conclusion
    D. Reconnaissance

12. Joe is a security engineer for a firm. His company downsizes, and Joe discovers he will be laid off within a short amount of time. Joe plants viruses and sets about destroying data and settings throughout the network, with no regard to being caught. Which type of hacker is Joe considered to be?

    A. Hactivist
    B. Suicide hacker
    C. Black hat
    D. Script kiddie

13. Elements of security include confidentiality, integrity, and availability. Which technique provides for integrity?

    A. Encryption
    B. UPS
    C. Hashing
    D. Passwords

14. Which of the following best describes an effort to identify systems that are critical for continuation of operation for the organization?

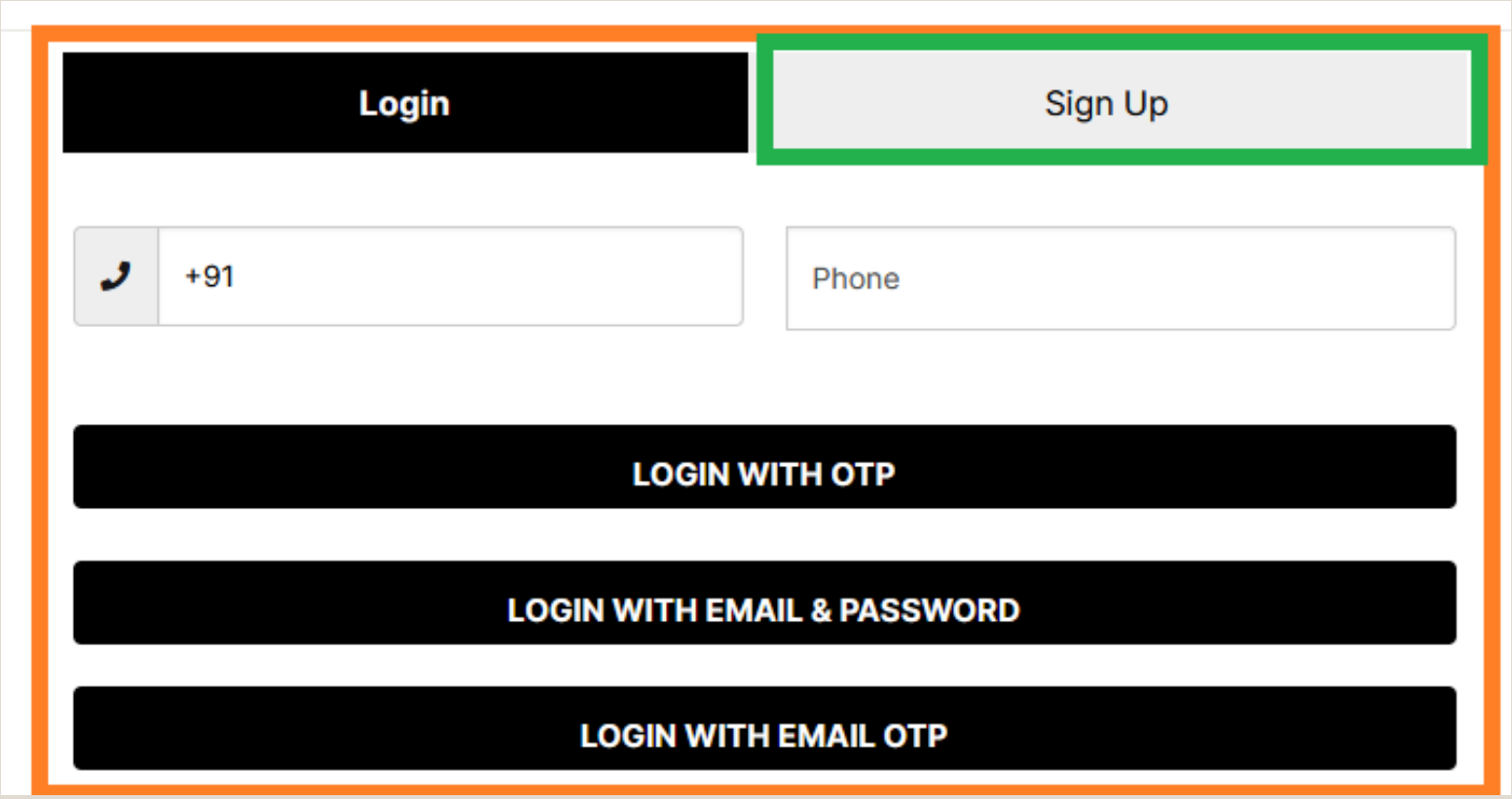
A. BCP
B. BIA
C. MTD
D. DRP

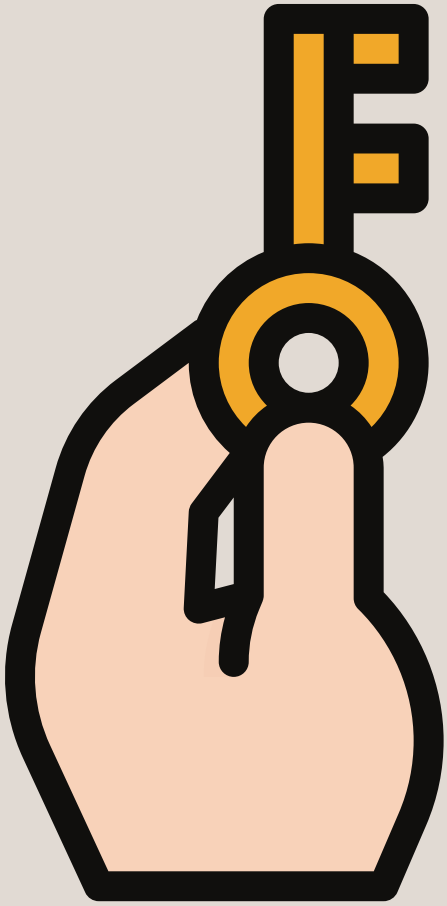
HOW TO GET COMPLETE PDF EBOOK

Pay Paytm

कोई भी **2 Ebooks** खरीदने पर **20%** डिस्काउंट- **India20**

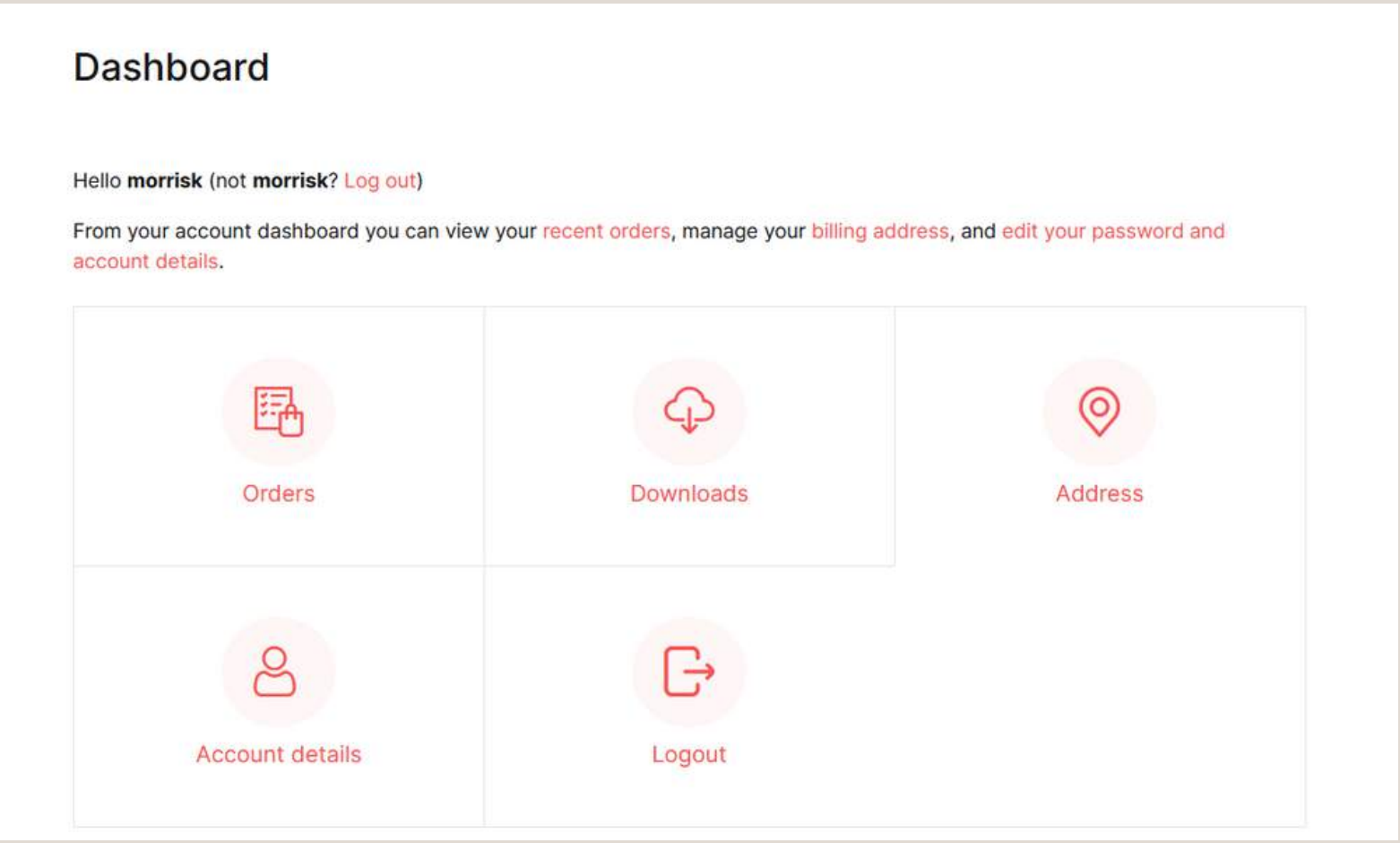
Buy Now पर क्लिक करने पर आपको **चेकआउट पेज** पर लॉगिन फॉर्म पर पहिले ईमेल से लॉगिन करना होगा।





Login Succesfull के बाद आपको पेमेंट करके Ebooks वही से डाउनलोड कर सकते है।

उसके बाद आप **My Account** पेज पर जाकर **Download** में Ebooks डाउनलोड कर सकते है।



Thank you